# Guida all'autodifesa digitale

- online -

Contrabbandiera

# Prefazione alla terza edizione

Meno di un anno dopo la pubblicazione dell'ultima edizione online della Guida, ci siamo già dovuti apprestare a prepararne un'altra. Sia per offrire una nuova edizione cartacea, sia per seguire l'evoluzione dei software raccomandati e quella dell'avverso panorama legislativo.

Non andremo qui a ripetere ciò che abbiamo scritto nella prefazione del primo volume: la tendenza è quella di rendere legale e normale la sorveglianza a 360 gradi. Per ciò che riguarda internet, un esempio evidente in Francia è la criminalizzazione della consultazione "abituale" dei siti web "che fanno apologia di terrorismo"[1], cosa che ha già mandato in prigione due persone: il primo si definiva un "apprendista giornalista"[2] mentre il secondo ha detto di agire per curiosità[3]. I due si sono beccati due anni di prigione. Questo reato è stato depenalizzato dal Consiglio Costituzionale[4] all'inizio di febbraio 2017, ma reintrodotto soltanto 18 giorni più tardi[5].

Sempre in Francia, diverse persone sono state condannate per la pubblicazione di articoli accusati di fare "apologia di terrorismo". Il rapporto Freedom of the net del 2015 riporta che "a Nantes un sedicenne è stato arrestato per aver condiviso su Facebook una vignetta legata all'attacco di Charlie Hebdo. La caricatura in questione prendeva in giro la copertina di

---

1 République française, 2016, *loi n. 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.*

2 Le Monde.fr, 2016, *Deux ans de prison ferme pour consultations répétées de sites djihadistes dans une bibliothèque* [tamuvo.vado.li].

3 Le Monde, 2016, *A Chartres, deux ans de prison ferme pour consultation de sites terroristes* [casano.vado.li].

4 Conseil constitutionnel, 2017, *Communiqué de presse - 2016-611 QPC* [cozaza.vado.li].

5 République française, 2017, *loi n. 2017-258 du 28 février 2017 - art. 24.*

luglio 2013 di Charlie Hebdo, pubblicata dopo il massacro di centinaia di egiziani che manifestavano contro il vecchio presidente islamista Mohamed Morsi e rappresentava un uomo mussulmano che reggeva il Corano per proteggersi dai proiettili e sopra c'era scritto "questo non ferma i proiettili". L'artista Dedko ha sostituito il corano con il giornale di Charlie Hebdo e l'uomo mussulmano con uno dei suoi disegnatori. Diverse voci hanno accusato le autorità francesi di usare due pesi e due misure per i casi di libertà di espressione[6].
Insomma, la protezione dell'intimità e della libertà d'espressione su internet sono più che mai d'attualità.
Questa nuova edizione include un nuovo caso d'impiego nella condivisione dei documenti riservati attraverso internet.
Riguardo ai software, il mese di giugno 2017 ha visto l'uscita della nuova versione di Debian, battezzata "Stretch" e anche la versione 3.0 del sistema live Tails, d'ora in avanti basato su "Stretch". Questo aggiornamento ha portato numerosi cambiamenti tanto a livello grafico, quanto nei software proposti. Abbiamo dunque dovuto rivedere le cose per correggere gli howto su questi nuovi sistemi. Questo ha portato all'aggiunta del programma OnionShare e all'arricchimento del programma OpenPGP con la cifratura e decifratura dei documenti.
Grazie a questa revisione, speriamo che le pagine che seguono vi siano d'aiuto durante la vostra traversata della giungla digitale...almeno, fino al prossimo aggiornamento...

---

6 Freedom House, 2015, *Freedom Of The Net: Privatizing Censorship, Eroding Privacy, p. 317* [sepito.vado.li].

# 0 | Prefazione

Il primo tomo di questa Guida ci ha fornito qualche informazione di base sul funzionamento di un computer *offline*, evidenziare cosa possono rivelare alle persone che lo utilizzano, proporre dei casi concreti sul loro utilizzo e infine delle "ricette" associate alle problematiche sollevate.
Come annunciato, questo secondo libro s'interesserà all'utilizzo di computer *online*. Vasto programma... perché se un'immersione tra i misteri di queste macchine così familiari si è già rivelata una storia complessa, cosa succederà se ora ci proponiamo di connettere dei computer tra di loro?
Ricordiamoci fin da ora che un computer connesso resta prima di tutto un computer; la (ri)lettura del primo tomo è dunque un prerequisito essenziale per comprendere tutte le sfaccettature della sicurezza in rete.
Nonostante tutto, nei Paesi ricchi l'utilizzo di internet fa ormai parte della cultura e dei costumi dei nostri giorni. Consultare le email, scaricare documenti, ottenere delle informazioni online sono per molti dei gesti quotidiani. Ciascuna persona potrebbe dire che in una certa maniera *sa* che cosa sia internet. Ammettiamo piuttosto che molti di noi sono capaci di adoperarlo per un utilizzo comune.
Il nostro scopo, in questo secondo volume, non sarà quello di definire nei più minuziosi dettagli che cosa sia internet. Piuttosto sarà quello di fornire qualche elemento di comprensione sufficiente per permettere di *navigarci* – ambiguità del termine che rimanda sia alla "navigazione sul web" che alla possibilità di orientarsi in uno spazio complesso con l'aiuto di strumenti adatti; o con il ritorno del sestante e della bussola...

Cominciamo dall'inizio. Internet è una rete. O piuttosto, è un insieme di reti connesse tra di loro, a partire da un'oscura applicazione militare, che si è estesa per decenni nel mondo intero. Rete che ha visto il moltiplicarsi di applicazioni, di usi e di utenti, di tecnologie e di tecniche di controllo.
Si è disquisito all'infinito sulla "nuova era" che stava nascendo, sulle presunte possibilità di orizzontalità e di trasparenza nella diffusione di informazioni e di risorse, e anche, tra le organizzazioni collettive che si sono affidate a questa nuova tecnologia, dell'aiuto che avrebbe fornito alle lotte politiche.
Tuttavia, dato che il potere non ama ciò che può sfuggirgli, si è sviluppato – parallelamente alla sua diffusione – un aumento delle tecniche di controllo, di sorveglianza e di repressione, con conseguenze che si fanno via via sempre più sentire.
Durante il 2011, per la prima volta, alcuni governi hanno organizzato la disconnessione dalla rete globale della quasi totalità della loro popolazione.
I dirigenti egiziani e iraniani, è di loro che stiamo parlando, hanno stimato che per meglio contenere le rivolte che avvenivano nei propri Paesi, avevano tutti gli interessi di limitare al massimo le possibilità di comunicazione della rete e al contempo tempo hanno cercato di organizzare la sorveglianza e il monitoraggio su internet. Il governo iraniano ha messo in piedi un sistema di analisi del traffico, ha chiesto risorse significative per monitorare alcune persone, note o meno, ha mappato le loro relazioni e successivamente le ha condannate perché avevano usato la rete per organizzarsi.
Un altro esempio: dopo l'apertura di una versione cinese di Google[1] nel 2006, l'azienda ha accettato piuttosto docilmente la politica del governo cinese di filtraggio dei risultati di ricerca.
Metodi simili sono stati usati anche dai cosiddetti Paesi democratici. Come ad esempio quando, nel 2011, dopo diverse gior-

1 Wikipedia, *Google China.*

nate di scontri a Londra, due giovani inglesi sono stati condannati a quattro anni di prigione[2] per aver lanciato un appello su Facebook sulle mobilitazioni nel loro quartiere, nonostante questo appello poi non avesse avuto un seguito effettivo.
E ancora: le rivelazioni di Edward Snowden[3] sullo stato di sorveglianza elettronico organizzato dalla NSA[4] su scala mondiale, hanno reso decisamente credibili le ipotesi dei più pessimisti.
A partire da ciò, sembra indispensabile prendere coscienza che l'utilizzo di internet, così come quello dell'informatica in generale, è tutto tranne che innocuo.
Ci espone alla sorveglianza e alla repressione: l'obiettivo principale di questo secondo tomo è permettere a chiunque di comprendere quali siano i rischi e i limiti associati all'utilizzo di internet e anche di fornire degli strumenti per fare delle scelte chiare in merito al suo utilizzo. Delle scelte che possano permettere di complicare il lavoro dei sorveglianti, di aggirare dei dispositivi di censura, di elaborare strumenti e infrastrutture in maniera autonoma. Un primo passo verso il riprendere il controllo di tecnologie che sembrano destinate a sfuggirci. Un'ambizione quest'ultima che tuttavia va ben oltre gli obiettivi di questa guida.
Eccoci allora di nuovo in viaggio tra le acque torbide del mondo digitale. La nostra traversata si svolgerà in tre parti, la prima spiegherà il contesto e le nozioni di base che permetteranno una comprensione generale; la seconda tratterà i casi più comuni e, infine, una terza parte descriverà precisamente gli utensili e il loro uso necessario all'implementazione delle policy di sicurezza proposte.

---

2 Le Figaro, 2011, *Émeutes à Londres: Deux jeunes condamnés à quatre ans de prison* [cegeci.vado.li].

3 Wikipedia, *Edward Snowden.*

4 National Security Agency, agenzia del dipartimento della difesa degli USA, incaricata della raccolta e analisi di dati stranieri e della protezione dei dati statunitensi.

PRIMA PARTE

# Comprendere

Nel primo volume della Guida all'autodifesa digitale abbiamo iniziato spiegando in che misura l'uso del computer potrebbe rappresentare una minaccia per la nostra intimità nel mondo digitale, soprattutto in relazione ai dati affidati. Immergersi nel mistero di queste macchine apparentemente così familiari si era già rivelato un po' complesso: cosa succederà ora che proponiamo di connetterci a internet, cioè di collegare il nostro computer ad altri computer, sui quali abbiamo poco o nessun controllo? Adesso dobbiamo quindi insistere sul fatto che un computer connesso è prima di tutto un computer; la (ri)lettura del primo volume è quindi un prerequisito essenziale per comprendere questo secondo e tutti gli aspetti della sicurezza online.

***Parigi, ottobre 2010***

*Questa mattina Alice è arrivata in anticipo al lavoro. È impiegata a La Reboute, un'azienda di vendite di abbigliamento per corrispondenza che si trova all'ultimo piano dell'edificio di via Jaurès: «Fiiuuuu, 18° piano, fortuna che l'ascensore è stato riparato!». Entra nel suo ufficio, si china e preme sul bottone di accensione del computer.*
*Sullo schermo appare una piccola finestra. «Connessione alla rete stabilita». Prima di mettersi al lavoro, Alice vuole controllare le sue email. Clicca sull'icona del browser, provocando l'apertura di una finestra che rimane vergine qualche millisecondo prima di mostrare la homepage di Google.*
*Mentre si gode mentalmente "Google speciale Halloween", Alice sposta il puntatore del mouse e fa clic sul collegamento.*
*Una volta che la pagina si è caricata, ci entra utilizzando il suo utente e password, poi clicca su Gmail.*
*Da qualche parte in una stanza buia affollata di computer, un hard disk si attiva.*

*Pochi secondi dopo aver aperto il browser web, Alice inizia a sfogliare la sua casella di posta.*
*Consulta un'email ricevuta dal sito «lebuoneoccasioni.fr», il suo sguardo è attirato da un link che compare nella colonna di destra: «Guarda, qualcuno vende lo stesso modello di macchina fotografica che cercavo... giusto all'angolo della strada. Dovrei farci un salto.»*
*«Ah sei qui?»*
*La voce alle spalle di Alice le fa fare un leggero balzo. È Benoît, un collega.*
*«Sì, mi sono svegliata prima rispetto al solito, ho preso la RER alle 7.27 invece che alle 7.43. Sto dando un'occhiata veloce alle e email prima di iniziare. Aspetto la conferma di una prenotazione di un biglietto per quest'inverno, alle Baleari.»*
*«Vacanze al sole! ...ne hai ancora per molto?»*
*Benoît ha l'aria stressata.*
*«No, no, ho quasi finito. Perché?»*
*«Beh, se non ti dispiace, prenderei in prestito la tua postazione per due minuti... La mia è offline da ieri, sto aspettando che arrivi il nuovo responsabile informatico per risolvere.»*
*Non appena si siede, Benoît fa clic nervosamente sulla barra degli indirizzi del browser e inserisce direttamente l'indirizzo del blog su cui vengono regolarmente pubblicate informazioni sui personaggi politici del suo quartiere.*
*Non gli piace andare su Google per le sue ricerche, quindi l'ha memorizzato. Non si sa mai, questo potrebbe evitare gli spioni. Aprendo una seconda scheda, inserisce anche l'indirizzo senza registrazione, cerca la sua casella di posta e si connette. Figata, eccolo! Il documento relativo ai conti bancari in Svizzera del sindaco del suo distretto, signor Alavoine! Benoît scarica immediatamente il documento e lo apre nell'editor di testo. Lo analizza rapidamente ed elimina alcune informazioni che è meglio non lasciare. Dopo aver inserito il nome utente e la password per connettersi al blog, Benoît copia e incolla il*

*contenuto del documento dalla sua casella di posta e fa clic su Invia.*
*«Spero che questo ispiri altre persone!»*
*Soddisfatto di essere riuscito ad inviare il suo documento, Benoît si alza velocemente e restituisce la postazione ad Alice.*
*«Andiamo a prendere un caffè?»*

## *Novembre 2010. Sede de La Reboute*

*Arrivato al lavoro, Samuel Coustant, amministratore delegato de La Reboute, inizia a dare un'occhiata alla posta ricevuta mentre beve il suo caffè.*
*Una convocazione dalla stazione di polizia. Per una volta, c'è qualcos'altro oltre le fatture! Senza dubbio un errore o un sondaggio di quartiere?*
*Samuel pensa di non avere nulla da nascondere, quindi non deve preoccuparsi. Si reca quindi in questura il giorno della convocazione.*
*«Sig. Coustant? Salve, vorremmo farle alcune domande in merito a un reclamo per diffamazione...»*

## *Più tardi, lo stesso giorno. Ufficio di Alice*

*«Pronto? Risorse Umane de La Reboute, sono Alice, mi dica.»*
*«Buongiorno, sono il Sig. Coustant. Ascolti, sono stato due ore in commissariato. Sono stato interrogato su dei documenti bancari pubblicati su internet che coinvolgono un certo Sig. Alavoine, Sindaco del X municipio, di cui finora ignoravo l'esistenza. In più, durante la mia udienza, mi hanno mostrato un documento che li autorizzava a perquisire gli uffici di rue Jaurès.»*
*«Che storia! Ma cosa c'entra con il nostro ufficio?»*

*«È proprio per questo che la chiamo. Affermano che hanno tutte le prove che dimostrano che questi documenti sono stati pubblicati dal nostro ufficio. Ho detto loro che non sono stato io, che non avevo idea di cosa stavano parlando. Hanno fatto delle ricerche, contattato non so chi. Ma dicono che è stata aperta un'indagine e che andranno fino in fondo. Che troveranno i responsabili. Detto ciò, vorrei dirle che non mi sento tranquillo. Spero che lei non ne sia responsabile e che si tratti di un deplorevole errore.»*
*«Onestamente, sono la prima ad essere sorpresa, non vedo assolutamente cosa c'entro con questa storia, non so di cosa stiamo parlando.»*
*«Lo spero... Comunque, ora tocca alla polizia fare il proprio lavoro. La richiamerò se avrò novità.»*
*«Ok, farò lo stesso se chiamano qui.»*
*«Arrivederci.»*
*Alice posa il telefono, stordita. Si gratta la testa. Ma qual è questa storia di documenti bancari? Chi avrebbe potuto farlo?*

***Centrale di polizia, Parigi, poche settimane dopo***

*«Commissario Mathias?»*
*«Sì, sono io.»*
*«Agente Nerret. La chiamo per l'affaire Alavoine. Abbiamo ricevuto un fax dai colleghi tecnici e scientifici che hanno esaminato i computer sequestrati. Abbiamo qualcosa di nuovo.»*
*«Avanti, Nerret. La ascolto.»*
*«I colleghi alla fine hanno trovato il documento su uno dei computer. È stato scaricato dal browser e poi modificato. Ci sarebbe stata una connessione a una casella di posta il cui indirizzo corrisponde a una certa Alice, su Gmail, e poi ad un altro indirizzo di posta elettronica – no-log.org – poco prima della pubblicazione dei documenti offensivi.»*

*«Ah, molto bene. Ma non intenderete mica prendere l'elenco telefonico e interrogare tutte le Alice che lavorano a La Redoute?»*
*«No, prima la troveremo e poi useremo l'elenco telefonico!»*
*«Che simpatia, Ufficiale!»*
*«Chiederemo informazioni sia a Gmail che all'indirizzo nolog.org su queste caselle di posta. Da lì probabilmente potremo mettere le mani sulle persone responsabili di questa pubblicazione.»*
*«Bene, Nerret. Molto bene. Io mi occuperò di contattare il Procuratore. E tienimi aggiornato non appena ci sono novità.»*
*«Bene, Commissario. Buona giornata.»*

Questo per quanto riguarda il contesto. Questa piccola storia di fantasia potrebbe ricordarne altre, molto più reali. L'idea era semplicemente quella di mostrare quanto sia facile e veloce esporsi connettendosi anche solo per poco tempo a internet, e questo senza che sia necessaria alcuna forma di sorveglianza mirata.
Per sapere poi quali tracce digitali ci permettono di risalire ad Alice e Benoît, uno degli obiettivi di questo secondo volume è appunto fare luce su questi punti. E di segnalare poi, ancora una volta, alcune strategie per proteggersi dagli attacchi, mirati o meno.

# 1 | Nozioni di base sulle reti

Internet non è uno spazio virtuale, una nuvola astratta di informazioni dove puoi trovare qualsiasi cosa. In ogni caso, non è solo quello.
Ciò che viene chiamato internet è soprattutto un insieme di reti[1]. Milioni di reti, aggregate in diversi decenni e in modo più o meno caotico; gestite da aziende, università, governi, associazioni e privati cittadini; milioni di computer e materiali di tutti i tipi, collegati tra loro da un'ampia varietà di tecnologie: dal cavo in rame, alla fibra ottica, al wireless.
Ma per noi, dietro il nostro piccolo schermo, internet è soprattutto ciò che ci permette di fare: visitare siti web, inviare email, chattare con persone o scaricare file. Nuove applicazioni appaiono costantemente e solo l'immaginazione umana sembra limitarne le possibilità.
Capire come funziona internet e come proteggerci è quindi indagare un minimo questa complessità, per capire come questi materiali comunicano tra loro, ma anche come funzionano le varie applicazioni che vi vengono utilizzate.

## 1.1 Più computer connessi insieme

Fin dall'inizio della storia dell'informatica, in particolare nel lavoro accademico e militare, è apparso necessario garantire che i computer potessero condividere risorse o informazioni e questo sentimento si è fatto sempre più forte. Così sono nate le reti di computer: inizialmente erano macchine che venivano prima assembrate insieme in un luogo piccolo, di solito un'università, un'azienda o un sito militare, e poi collegate tra loro.

1 Per una spiegazione in 5 minuti, in francese: Rémi explique, 2015, *Internet! Comment ça marche?* [modoge.vado.li].

Negli Stati Uniti alla fine degli anni 60 è stato creato ARPANET (Advanced Research Projects Agency Network), una rete che collegava le università di tutto il Paese. Per la sua implementazione e miglioramento, sono state inventate molte delle tecniche utilizzate oggi con internet. La sua nascita è fortemente legata a quella del software libero e opera su simili principi di apertura e trasparenza[2], il che non ne impedisce lo sviluppo per soddisfare altri tipi di esigenze, come quelle militari.
Le varie reti di computer sono state collegate nel tempo, costituendo così gradualmente internet, che si è sviluppata in modo significativo dagli anni 90 in poi.
Da allora sempre più oggetti – la cui funzione primaria non è quella di essere un computer – sono stati connessi:

- telecamere di sorveglianza[3]
- radar stradali[4]
- Terminali PMU[5]
- TV[6]
- frigoriferi[7]
- apparecchiature mediche[8]

---

2 Secondo Benjamin Bayart, “non possiamo separare internet dal software libero” perché sono apparsi nelle stesse date, avevano gli stessi giocatori e avevano una crescita e un funzionamento simili. Benjamin Bayart, 2007, *Free internet, or Minitel 2.0?*, Conferenza all’8° Free Software World Meetings di Amiens [lunivi.vado.li].

3 Jérôme, 2012, *Telecamere IP: il difetto del voyeur colmato* [sezale.vado.li].

4 Korben, 2013, *Radar educativi in balia dei pirati?* [zinumo.vado.li].

5 AFP, 2012, *PMU: 5 persone arrestate a nord di Marsiglia per aver violato i terminali* [biroma.vado.li].

6 Fabien Soyez, 2013, *Vita privata: TV connessa, la spia perfetta* [madomi.vado.li].

7 Camille Kaelblen, 2016, *Il tuo frigorifero connesso è il punto di ingresso ideale per gli hacker?* [gunoza.vado.li].

8 Gilles Halais, 2012, *Un hacker ha scoperto come hackerare i pacemaker a distanza* [dopana.vado.li].

- giocattoli per bambini[9]
- automobili[10]
- ...

Alcune persone parlano addirittura di “internet of shit”[11] per mostrare l’assurdità del numero di oggetti che sono stati collegati alla rete.

### 1.1.1 Una rete di computer

“Una rete è un insieme di nodi [...] collegati l’uno con l’altro da appositi canali di comunicazione”[12].
In una rete di computer, i nodi sono computer[13]. Si tratta insomma di un insieme di computer collegati tra loro da cavi, onde, ecc[14].
I computer che fanno parte dei nodi non sono tutti simili ai personal computer, desktop o portatili che usiamo quotidianamente. Alcuni sono pensati per svolgere funzioni particolari all’interno della rete. Lo “scatolotto” attraverso il quale la maggior parte di noi accede a internet è un piccolo computer; ma, allo stesso modo, anche i server su cui sono memorizzati i siti web sono computer. Altri tipi di computer specializzati potrebbero ancora essere aggiunti a questo elenco: ne scopriremo alcuni nelle pagine seguenti.

---

9 Sandrine Cassini, 2015, *VTech, le vittime della pirateria* [difovu.vado.li].
10 HuffingtonPost, 2015, *Un’auto hackerata a distanza dagli hacker* [lilugi.vado.li].
11 Guillaume Ledit, *Su Twitter, “internet of shit” mette in ridicolo l’internet delle cose... di merda* [tosube.vado.li].
12 Wikipedia, *Reti di computer.*
13 Tomo I, cap. 1
14 Cap. 1.1.3

### 1.1.2 La scheda di rete

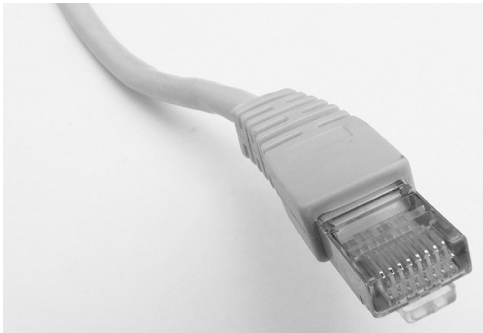
Nonostante le loro differenze, tutti i computer collegati a una rete hanno necessariamente una cosa in comune: oltre all'hardware minimo che compone un computer[15], devono avere almeno una periferica[16] che viene utilizzata per connettersi alla rete. Si chiama "scheda di rete". Consente di stabilire il collegamento con altri computer[17]. Al giorno d'oggi, su un qualsiasi personal computer si trovano integrate diverse schede di rete (per esempio una via cavo e una wi-fi).
Ogni scheda di rete ha un indirizzo hardware, che la identifica in modo più o meno univoco. Nella tecnologia domestica via cavo (Ethernet) e in quella wireless (wi-fi), l'indirizzo hardware è chiamato "MAC address". Il MAC address fornito con la scheda è progettato in modo tale che la probabilità che due schede di rete abbiano lo stesso indirizzo hardware sia molto bassa[18], il che porta a problemi di anonimato, come vedremo in seguito[19].

### 1.1.3 Vari tipi di collegamenti

I modi più comuni per collegare i personal computer a una rete sono collegare un cavo, noto come cavo Ethernet, o utilizzare le onde radio, con il wi-fi.
Ma al di là della nostra presa telefonica, le nostre comunicazioni su internet vengono trasportate con molti altri mezzi. Esistono diversi supporti per la trasmissione di informazioni:

---

15 Tomo I, cap. 1
16 Tomo I, cap. 1.2.5
17 Cap. 1.1.3
18 Un MAC address ha la forma di una sequenza di 12 cifre esadecimali (da 0 a 9, a per 10, b per 11 e così via fino a f per 15) come, per esempio, `00: 3a: 1f: 57: 23: 98`.
19 Cap. 2.2

cavo in rame, fibra ottica, onde radio, ecc. Dalla trasmissione modem[20] degli anni 90 alla fibra ottica[21] utilizzata per le connessioni intercontinentali, passando per l'ADSL[22] negli anni 2000, ognuna di queste presenta caratteristiche differenti, in particolare in termini di flusso di informazioni (la larghezza della banda), di costi di installazione e di manutenzione.
Queste diverse tecnologie non hanno gli stessi punti deboli per quanto riguarda la riservatezza delle comunicazioni che vi transitano o delle tracce che lasciano: sarà sicuramente più facile intercettare un segnale radio da lontano, che ricavare un indizio dalla luce che passa all'interno di una fibra ottica.

*Un connettore Ethernet RJ-45 standard*

20 Modem è l'acronimo di *MOdulator-DEModulator*: consente la trasmissione di dati digitali su un canale [tomo I, cap. 1.2.2 "Il processore"] consentendo la trasmissione del suono, ad esempio una linea telefonica.
21 Una fibra ottica è un filo costituito da un materiale trasparente utilizzato per trasmettere dati sotto forma di impulsi luminosi. Ciò consente la trasmissione di grandi volumi di informazioni, anche su lunghe distanze.
22 ADSL (per Asymmetric Digital Subscriber Line) o VDSL (per Very-high-bit-rate Digital Subscriber Line) è una tecnologia che consente la trasmissione di dati digitali su una linea telefonica indipendentemente dal servizio telefonico.

## 1.2 Protocolli di comunicazione

Affinché delle macchine possano parlarsi, non è sufficiente che siano interconnesse, ma devono anche saper parlare una lingua comune, che nel nostro caso è chiamata "protocollo di comunicazione". La maggior parte dei linguaggi utilizzati dalle macchine su internet sono definiti con precisione in documenti pubblici: è questo che consente alle reti, ai computer e ai vari software di lavorare insieme, purché rispettino gli standard. È il concetto di "interoperabilità".
Il funzionamento di internet si basa sull'utilizzo di varie convenzioni, dette anche "protocolli", che soddisfano diverse esigenze: scaricare un file, inviare una email, consultare un sito web, ecc.
Per semplificare le cose, descriveremo in dettaglio questi diversi protocolli di seguito classificandoli in tre categorie: protocolli fisici, protocolli di rete e infine i protocolli applicativi[23].
E per comprendere appieno cosa c'è di meglio di un'analogia? Confronteremo quindi il viaggio delle nostre informazioni scambiate attraverso internet con la consegna di una cartolina le cui tappe, dal centro di smistamento postale alla cassetta delle lettere, corrispondono ai diversi computer interconnessi.

### 1.2.1 Protocolli fisici

Per consegnare la nostra cartolina in sicurezza, possono essere utilizzati diversi mezzi di trasporto: aereo, nave, camion o anche bicicletta. Ciascuno di questi deve far fronte ad un certo numero di normative: codice della strada, traffico aereo, idiritto marittimo, ecc.
Allo stesso modo, su internet, le varie tecnologie hardware

23 . In realtà è un po' più complicato di così, per maggiori dettagli vedere: Wikipedia, *Protocolli di comunicazione*.

utilizzate[24] implicano l'uso di convenzioni differenti. Parliamo in questo caso di "protocolli fisici".

### 1.2.2 Protocolli di rete

Non basta saper guidare per riuscire a consegnare la nostra cartolina: si deve anche conoscere come leggere un codice postale o avere una certa dimestichezza con il quartiere per raggiungere il nostro destinatario o il centro di smistamento più vicino.
È qui che entrano in gioco i "protocolli di rete": il loro obiettivo è consentire l'instradamento delle informazioni tra più macchine distanti tra di loro, indipendentemente dalle connessioni fisiche.
Il protocollo di rete più famoso è il protocollo IP[25].

### 1.2.3 Protocolli applicativi

Utilizziamo spesso internet per accedere a pagine web, ovvero ad un insieme di pagine accessibili su un server[26] che consultiamo da un browser web. `https://guide.boum.org` è un esempio di un sito web. Il linguaggio comune confonde spesso il web con internet, utilizzando ad esempio espressioni come "andare su internet". Ma il web è solo uno dei tanti utilizzi possibili di internet.
Esistono moltissime applicazioni che utilizzano internet, e che la maggior parte degli utenti non sa di stare usando. Oltre al web, ci sono le email, la messaggistica istantanea, il trasferimento di file, le valute digitali come Bitcoin, ecc.

---

24 Cap. 1.1.3
25 Cap. 1.2.5
26 Cap. 1.5

Allo stesso modo ci sono anche diversi protocolli che, pur utilizzando internet, *non* fanno parte del web. Per esempio:

- SMTP, POP, IMAP utilizzati nella posta elettronica[27], di cui esistono anche versioni cifrate IMAPS, POPS, SMTPS;
- Skype, Yahoo Messenger, Signal, IRC e XMPP utilizzati nella messaggistica istantanea;
- BitTorrent, un protocollo di condivisione di file peer-to-peer.

Una persona che ha sufficienti conoscenze di programmazione può creare autonomamente un nuovo protocollo e quindi un nuovo modo di usare internet.
Ogni applicazione internet utilizza quindi un particolare linguaggio – detto "protocollo applicativo" – e inserisce il risultato nei pacchetti che vengono trasmessi dai protocolli di rete. Possiamo quindi paragonarlo alla lingua del testo della nostra cartolina: il mittente e il destinatario devono conoscere questa lingua, alle Poste invece non hanno bisogno di capire cosa c'è scritto nella cartolina, gli importa solo che contenga un indirizzo valido.
Di solito le cartoline non arrivano in busta chiusa, chiunque per strada le può leggere, mittente e destinatario sono visibili per chiunque. Allo stesso modo esistono anche diversi protocolli applicativi non cifrati[28]: anche in questo caso, il contenuto dei pacchetti è leggibile da tutti.
I protocolli non sono tutti trasparenti: alcuni sono aperti e accessibili (e quindi verificabili da chi lo desidera), altri utilizza-

27 C'è una notevole differenza nei protocolli utilizzati, che ha conseguenze in termini di riservatezza e anonimato, a seconda che si utilizzi una casella di posta tramite il proprio browser (webmail) o tramite un client di posta. Ne riparleremo presto [cap. 10.5].
28 Tomo I, cap. 5

no protocolli proprietari[29] scarsamente documentati. Risulta quindi difficile analizzare quali eventuali informazioni sensibili potrebbero essere contenute nei dati scambiati.
Skype ad esempio funziona come un vero e proprio buco nero: fa quello che dice fare (permetterti di comunicare), ma probabilmente fa anche molto altro. In particolare si è scoperto che il contenuto dei messaggi viene analizzato, ed eventualmente censurato[30], e che tutti gli indirizzi web inviati tramite chat vengono inoltrati a Microsoft[31].

### 1.2.4 Incapsulamento

In realtà, durante una comunicazione vengono utilizzati contemporaneamente protocolli diversi, ciascuno dei quali ha un ruolo nell'instradamento delle informazioni.
Di solito, si usa rappresentare questi diversi protocolli come strati che si sovrappongono.
Quando comunichiamo tramite una cartolina, la nostra comunicazione si basa sulla scrittura, sulla consegna da parte delle Poste, che a sua volta si basa su diversi mezzi di trasporto.
Un applicativo internet utilizzerà invece un preciso protocollo applicativo e la comunicazione verrà instradata attraverso l'utilizzo di protocolli di rete, navigando tra le varie infrastrutture nel rispetto dei protocolli fisici in vigore.
Si parla quindi di "incapsulamento": i protocolli applicativi sono incapsulati in protocolli di rete, a loro volta incapsulati in protocolli fisici.

---

29 Tomo I, cap. 4
30 Slate.com, 2013, *«Lance des œufs», «cinéma coquin». La liste des mots surveillés par Skype en Chine* [tepilo.vado.li].
31 Jürgen Schmidt, 2013, *Skype's ominous link checking: Facts and speculation* [nulige.vado.li].

*Protocollo incapsulato*

### 1.2.5 Ancora dettagli sul protocollo IP

È interessante notare che, a differenza dei protocolli fisici e applicativi, i protocolli di rete sono relativamente universali. I protocolli fisici si evolvono con il progresso della tecnologia via cavo o wireless. I protocolli applicativi si evolvono con lo sviluppo di nuove applicazioni: web, email, chat, ecc. Tra questi due livelli, è a partire dagli anni 80 che si comincia a instradare i pacchetti, per sapere dove andare e come attraverso milioni di reti: è il protocollo IP (Internet Protocol Address).

**Pacchetti**
Nel protocollo IP le informazioni vengono sminuzzate e confezionate "in pacchetti", sui quali sono scritti in particolare l'indirizzo di spedizione e di destinazione. Questa "etichetta" su cui vengono scritte le informazioni utili per l'instradamento dei pacchetti, sia in uscita che in entrata, è l'intestazione (he-

ader). I pacchetti vengono trasmessi indipendentemente l'uno dall'altro, a volte utilizzando percorsi diversi e riassemblati in seguito, una volta giunti a destinazione. Questo è il motivo per cui viene usato anche un altro protocollo, chiamato TCP (Transmission Control Protocol): in questo modo si garantisce che tutti i pacchetti siano arrivati e nell'ordine corretto. Oltre al TCP esistono però anche altri protocolli diversi che gestiscono il trasporto dei pacchetti[32].

**Indirizzo IP**

Qualsiasi computer connesso alla rete deve avere un indirizzo, utilizzato per l'invio dei pacchetti. L'indirizzo IP deve essere univoco all'interno di una rete: se più computer avessero lo stesso IP, la rete non sarebbe in grado di sapere a chi inviare pacchetti.

Possiamo mettere a confronto l'indirizzo IP con un numero di telefono: ogni apparecchio deve avere un numero telefonico per poterlo chiamare. Se più telefoni avessero lo stesso, ci sarebbe un problema.

Gli indirizzi utilizzati fin dagli albori di internet si presentano sotto forma di quattro numeri, separati da un punto: si parla di indirizzi IPv4 (Internet Protocol versione 4). Un indirizzo IPv4 è fatto così: `203.0.113.12`.

Il protocollo IPv4 è stato definito all'inizio degli anni 80 e consente l'assegnazione di un massimo di 4 miliardi di indirizzi. A quel tempo, non si immaginava che un giorno internet sarebbe stato accessibile al grande pubblico e si credeva che 4 miliardi sarebbero bastati.

---

32 Un altro protocollo comunemente utilizzato per la trasmissione è UDP (User Datagram Protocol), soprattutto quando è necessario trasmettere dati molto velocemente, anche se significa perderne una parte. Nel caso della telefonia internet, ad esempio, una serie di blocchi o pause nella comunicazione causati da una leggera perdita di dati, sono per lo più impercettibili dagli utenti e non è troppo diverso da una classica chiamata con il telefono.

Negli anni 90, per far fronte all'incombente carenza di indirizzi, IETF[33] iniziò a lavorare su IPv6 (Internet Protocol versione 6). Dal 2011 però è diventato un problema reale per i nuovi operatori poter ottenere un IPv4. Il protocollo IPv6 è stato quindi gradualmente implementato tra gli operatori (anche se ce ne sono di riluttanti). L'applicazione di IPv6 coinvolge degli interessi politici considerevoli[34], ma anche delle nuove problematiche di sicurezza[35]. Nel 2017 i due protocolli (v4 e v6) funzionavano in parallelo. Un indirizzo IPv6 ha il seguente aspetto: `2001: 0db8: 85a3: 0000: 0000: 8a2e: 0370: 7334`.
L'indirizzo IP è un'informazione estremamente utile per chiunque desideri monitorare ciò che sta accadendo su una rete, in quanto identifica in modo univoco un computer in un dato momento e – pur senza essere effettivamente una prova reale[36] contro una persona (un computer può essere utilizzato da più persone) – può tuttavia indicare l'origine geografica di una connessione, fornire indizi, avviare o confermare sospetti.

### 1.2.6 Porte

Possiamo utilizzare contemporaneamente diverse applicazioni dallo stesso computer: leggiamo le email scaricandole con Thunderbird, navighiamo tra siti web che ci interessano, mentre chattiamo con gli amici e ascoltiamo musica online. Ogni applicazione dovrebbe ricevere solo i pacchetti a essa destinati e che contengono messaggi in una lingua che comprende. Il

---

33 Wikipedia, *Internet Engineering Task Force.*

34 Una conferenza in francese di LDN (Lorraine Data Network) spiega la posta in gioco intorno al IPv6: taduza.vado.li.

35 Queste normative pongono nuove questioni relative all'anonimato in rete. Ne riparleremo più avanti. Florent Fourcot, 2011, *Journal IPv6 et conséquences sur l'anonymat* [leduto.vado.li].

36 Legalis, 2013, *L'adresse IP, preuve insuffisante de l'auteur d'une suppression de données sur Wikipedia* [muvopi.vado.li].

punto però è che un computer connesso alla rete ha un solo indirizzo IP. A questo indirizzo viene quindi aggiunto un numero che gli consentirà di inviare il pacchetto all'applicazione giusta. Questo numero lo scriviamo sul pacchetto, dopo l'indirizzo: questo è il numero di *porta*.
Per capire, confrontiamo il nostro computer con un edificio: l'edificio ha un solo indirizzo, ma ospita molti appartamenti e persone diverse. Il numero dell'appartamento scritto su una busta consente di inviare la posta al destinatario corretto. Lo stesso vale per i numeri di porta: consentono al server di inviare i dati all'applicazione corretta.
Per convenzione alcuni numeri di porta vengono assegnati a delle precise applicazioni. Quindi, quando il nostro browser vuole connettersi a un server web, sa che deve bussare alla porta 80 (o 443 nel caso di una connessione cifrata). Invece, per inviare un'email il nostro computer si connetterà generalmente alla porta 25 [37](o 465 se si tratta di una connessione cifrata).
Sul computer che stiamo utilizzando, ogni applicazione connessa a internet apre almeno una porta, sia che si tratti di un browser web, di un software di messaggistica istantanea, di un lettore musicale, ecc. Quindi, il numero di porte aperte durante la nostra sessione quotidiana su internet può essere molto alto e la sola chiusura del browser web non è sufficiente per interrompere tutte le connessioni che abbiamo effettuato attraverso la rete.

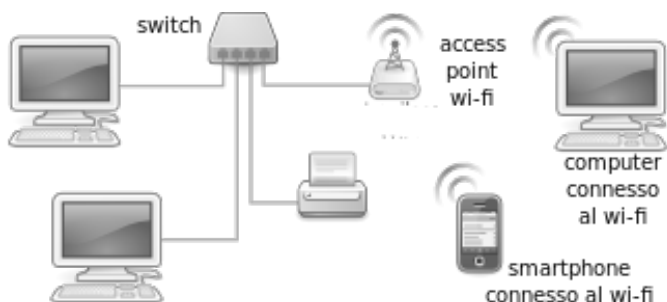
*Più porte aperte ci sono su un computer connesso alla rete, più ci sono punti dai quali è possibile infiltrarsi. Lo scopo di un* ***firewall*** *è quello di lasciare aperte solo le porte che abbiamo definito nella configurazione e rifiutare le richieste che arrivano ad altre porte.*

37 Cap. 1.5

## 1.3 Le reti locali

Esistono e possiamo creare reti senza internet. Le reti di computer sono apparse molto prima di internet: negli anni 60, i protocolli di rete come HP-IB[38] consentivano la connessione solo a un numero limitato di computer, facendo già funzionare le cosiddette "reti locali".

### 1.3.1 La rete locale, struttura di base di internet

Quando colleghiamo più computer insieme nello stesso edificio – casa, scuola, università, ufficio, ecc. – parliamo di una rete locale o LAN (Local Area Network). I computer possono quindi comunicare tra loro, ad esempio per scambiare file, condividere una stampante o giocare su una rete.
Le reti locali possono essere paragonate alle reti telefoniche interne di alcune organizzazioni (azienda, università).
Queste reti locali sono spesso costituite da diversi dispositivi che comunicano tra loro:

38 Wikipedia, *HP-IB*.

### 1.3.2 Switch e Access Point wi-fi

Per connettere le macchine ad una LAN, ciascuna sarà collegata ad una "presa multipla", tramite cavo o wi-fi. Spesso viene utilizzato uno "switch", una sorta di presa multipla intelligente: invece di trasmettere ogni pacchetto che arriva a *tutti* i computer della rete, uno switch legge l'indirizzo indicato sul pacchetto e lo invia solo alla corretta destinazione.
L'equivalente dello switch nelle reti wireless si chiama "Access point". Ciascun access point possiede un nome, che viene divulgato nell'ambiente circostante e mostrato nell'elenco delle reti wi-fi che la nostra scheda di rete vede.
Per riprendere il nostro esempio, lo switch è un po' come il postino: consegnerà la posta, in tutto il quartiere, a ciascun destinatario. Per fare ciò, lo switch ricorda l'elenco delle schede di rete , identificate dal loro indirizzo hardware[39], collegate ciascuna alla propria presa.
Così come l'accesso fisico a una macchina offre molte possibilità per recuperare le informazioni che ci sono dentro, avere accesso fisico a una rete permette, a meno di difese particolari, di farsi passare per una qualche macchina appartenente alla rete. Ciò rende possibile la raccolta di molte informazioni riguardo alle comunicazioni che transitano in quella rete, mettendo in atto quello che viene chiamato attacco Man in the Middle[40].
L'accesso fisico alla rete può avvenire attaccandosi con un cavo a uno switch, ma anche attraverso un access point wi-fi.

### 1.3.3 Indirizzi

Affinché le macchine collegate alla rete possano comunicare con il protocollo IP, ciascuna di esse deve avere un indirizzo

39 Cap. 1.1.2
40 Cap. 6.4.1

IP[41]. Per evitare di dover configurare indirizzo IP e parametri di rete a mano su ciascuna macchina, sono stati sviluppati dei programmi e dei protocolli che automatizzano questo passaggio durante la connessione a una rete. Ad esempio il protocollo DHCP[42] per IPv4 o NDP[43] (e SLAAC per IPv6[44]).
Per funzionare, questi software associano una scheda di rete, identificata tramite indirizzo fisico[45], a un certo indirizzo IP e tengono in memoria questa associazione. Questo tipo di software si trova in genere su un apparato di rete come lo switch, ma può anche risiedere altrove sulla rete locale. Questa associazione tra indirizzo IP e indirizzo fisico è utile soltanto all'interno della rete locale, perché è legata al protocollo fisico utilizzato al suo interno. Questa informazione non ha dunque alcun motivo tecnico per circolare su internet, eppure ci arriva lo stesso[46].

### 1.3.4 NAT e indirizzi riservati alle reti locali

Gli organismi di standardizzazione di internet si sono resi conto negli anni 90 che il numero di indirizzi IPv4[47] disponibili non sarebbe stato sufficiente per far fronte alla rapida crescita della rete. Per risolvere questo problema, alcuni intervalli di indirizzi sono stati riservati alle reti private, che non vengono utilizzate su internet: si tratta di "indirizzi privati"[48].

41 Cap. 1.2.5
42 Utilizzato nelle reti IPv4, DHCP sta per *Dynamic Host Configuration Protocol.*
43 Wikipedia, *Neighbor Discovery Protocol.*
44 Per attribuire un indirizzo statico: it.wikipedia.org/wiki/Indirizzo_IP
45 Cap. 1.1.2
46 Cap. 2.2
47 Cap. 1.2.5
48 In contemoranea, l'IETF lavora sulla versione 6 del protocollo IP che risolverebbe la penuria di indirizzi.

È per questo che la maggior parte degli "scatolotti" che assegnano gli indirizzi ai computer li fanno iniziare per con `192.168`[49] in IPv4, `fe80:` in IPv6. Varie reti locali possono utilizzare gli stessi indirizzi IP privati, a differenza degli indirizzi IP su internet, che devono essere univoci a livello globale.
I pacchetti che recano questo tipo di indirizzi non possono uscire dalla rete privata così come sono. Questi indirizzi privati vengono utilizzati solo all'interno della rete locale. La mia macchina, all'interno della rete locale ha come indirizzo IPv4 `192.168.0.12`, ma alle altre macchine con le quali comunicherà su internet sembrerà che abbia come indirizzo quello dello scatolotto che mi connette a internet (per esempio `203.0.113.48`): questo indirizzo si chiama "indirizzo pubblico". Lo "scatolotto" si farà carico di modificare i pacchetti di conseguenza, tramite un processo di traduzione che si chiama NAT (Network Address Translation).

## 1.4 Internet, reti interconnesse

Internet significa INTERconnected NETworks ovvero interconnessione di reti. Ciascuna di queste reti è chiamata "Autonomous System", o AS.

### 1.4.1 Gli Internet Service Provider

Gli Internet Service Provider (o ISP) sono organizzazioni che forniscono una connessione a internet tramite fibra ottica, onde elettromagnetiche (wi-fi, 4G o altre), una linea telefonica o un cavo. In Francia, i principali fornitori commerciali di

---

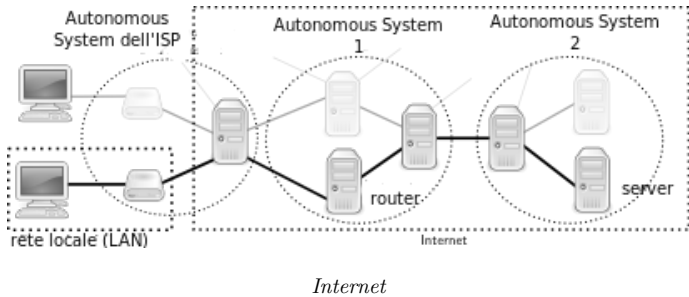
49 Gli intervalli di indirizzi privati sono definiti per convenzione in un documento denominato "RFC 1918". Includono, oltre agli indirizzi che iniziano con `192.168`, quelli che iniziano con `10` e da `172.16` a `172.31`.

accesso a internet per uso domestico sono Orange, Free, SFR o Numericable e esistono anche ISP associativi come membri della Federazione FDN.
Spesso un ISP gestisce la propria rete alla quale sono connessi gli "scatolotti" delle persone abbonate. Questa rete costituisce l'Autonomous System dell'ISP, che si fa carico di connetterlo con gli altri AS.
Per connettere la rete locale ad altre reti, è necessario un router, cioè un computer il cui ruolo è quello di inoltrare i pacchetti tra due o più reti.
Nel caso di una casa che debba essere collegata a internet, il ruolo di router lo ricopre uno "scatolotto". Lo definiamo modem-router, ed è composto da una scheda di rete collegata alla rete locale e da un modem ADSL o una porta per la fibra collegati alla rete del fornitore d'accesso a internet. È uno scatolotto che fa parte sia della rete locale che di internet: con IPv4, sarà l'indirizzo IP dello scatolotto ad essere visibile su internet su tutti i pacchetti che fa uscire dai computer della rete locale. Al contrario, con IPv6 tutte le macchine connesse alla rete avranno degli indirizzi pubblici che fanno parte di internet.
Lo "scatolotto" è un piccolo computer che al suo interno include un modem-router, i software che permettono di gestire una rete locale (per esempio il software che fa da DHCP[50]), uno switch Ethernet e/o wi-fi in modo da poterci attaccare vari computer, e a volte anche un decoder per la televisione, un hard-disk, ecc.

### 1.4.2 Gli Autonomous System

Un autonomous system (AS, sistema autonomo) è una rete coerente – solitamente di una singola entità o organizzazione

50 Cap. 1.3.3

– in grado di funzionare indipendentemente dalle altre reti.
Nel 2017, internet era formato dall'interconnessione di poco meno di 58.000 AS in tutto il mondo[51]. Un sistema autonomo tipico è la rete di un provider di servizi internet (ad esempio Free, SFR o tetaneutral.net). In questo caso, ciascuno "scatolotto" che serve a connettere una rete locale domestica a internet, fa anche parte della rete dell'ISP, che è a sua volta connessa ad altri Autonomous System e tutti insieme formano internet. Anche le organizzazioni che ospitano siti web (ad esempio Dailymotion, Google o Riseup) e quelle che gestiscono le "grandi dorsali" – come i cavi transatlantici, attraverso i quali passa gran parte del flusso di dati – dispongono dei propri Autonomous System.

*Internet*

Tuttavia internet non è una grande rete omogenea gestibile in modo centralizzato. È costituita piuttosto da una moltitudine di reti connesse tra loro, gestite da organizzazioni e aziende diverse e variegate, ciascuna con la propria funzione.
Tutte queste reti, infrastrutture e computer, non funzionano da soli: sono gestiti quotidianamente da persone, che vengono chiamate "amministratori o amministratrici di sistema",

51 Possiamo trovare delle statistiche carine sull'evoluzione degli AS su https://www.cidr-report.org/as2.0/

o “sys admin”[52]. Sono loro che si occupano dell’installazione, della manutenzione e dell’aggiornamento di queste macchine. Per fare ciò, hanno *necessariamente* accesso a una grande quantità di informazioni che risiedono sui computer di cui sono responsabili.
In termini di sorveglianza, gli interessi commerciali e gli obblighi legali degli Autonomous System variano notevolmente a seconda degli Stati e dei tipi di organizzazione coinvolti (istituzioni, società, associazioni, ecc.). Nessuno ha il pieno controllo di internet e la sua natura globale rende complicato qualsiasi tentativo di legislazione unificata. Non c’è quindi omogeneità di pratiche.

### Interconnessioni di reti

Nello stesso modo in cui abbiamo collegato la nostra rete locale all’Autonomous System del nostro ISP, quest’ultimo stabilisce delle connessioni con altre reti. In questo modo si possono passare le informazioni da un sistema autonomo a un altro.
È grazie a queste interconnessioni che possiamo comunicare con i vari computer che formano internet, indipendentemente dall’AS di appartenenza.

*Un routeur Avaya Secure Router 2330*

52 Del ruolo degli admin ne riparleremo più avanti.

Un router è un computer che collega e fa comunicare tra loro varie reti. Negli ISP i router sono accesi di continuo e assomigliano più a grandi scatole di pizza che a personal computer. Il loro principio di funzionamento resta però simile a quello degli altri computer, a cui è stato aggiunto qualche circuito specifico per trasportare molto velocemente i pacchetti da una rete all'altra.
Gli Autonomous System si mettono d'accordo tra loro per scambiarsi il traffico: si parla in questo caso di accordi di *peering*. Molto spesso, il peering è gratuito e lo scambio è equilibrato. Per raggiungere gli Autonomous System con i quali non si ha un accordo di peering, un operatore può avvalersi di un transit provider, ovvero qualcuno che può raggiungere l'intera internet e vende la connettività agli altri operatori[53].

A *proposito di scambio di traffico, esiste un principio che in teoria esclude ogni discriminazione, sulla fonte, sulla destinazione o sul contenuto trasmesso in rete. Si tratta della* Net Neutrality*. Questo principio garantisce agli utenti che non verrà utilizzata alcuna gestione del traffico internet volta a limitare l'accesso alle applicazioni e ai servizi distribuiti in rete. Ad esempio, limitare la visualizzazione o il download di video online. La Net Neutrality garantisce che i flussi informativi non siano bloccati, degradati o favoriti dagli operatori di telecomunicazioni, consentendone così il libero utilizzo[54]. In Francia, Quadrature du Net[55] e la Federazione FDN[56] difendono e promuovono la Net Neutrality.*

53 Loïc Komol, 2013, *Le peering: petite cuisine entre géants du Net* [vimuso.vado.li].

54 #DataGueule ha realizzato un video che spiega chiaramente la neutralità della rete e le questioni politiche associate [tageto.vado.li].

55 La neutralità della rete vista da Quadrature du Net: vetovi.vado.li.

56 Carta dei principi della Federazione FFDN: cigufo.vado.li.

## Punti di interscambio...

Gli operatori che forniscono le infrastrutture di rete hanno cominciato tirando cavi verso ogni router, per poi rendersi conto che si trattava di un bel po' di cavi e che occorrevano un sacco di soldi, e che in molti casi sarebbe stato parecchio più semplice se ciascuno fosse arrivato con il proprio cavo in un unico punto.
Esistono quindi dei punti in cui convergono molti Autonomous System per collegarsi tra loro. Ognuno di questi punti viene chiamato *punto d'interscambio* (*IXP* - internet Exchange Point): gli Autonomous System che vogliono utilizzarli ci si portano un cavo e ci installano i propri router. A causa della notevole quantità di traffico che li attraversa, questi luoghi sono di importanza strategica per gli Stati e per altre organizzazioni che vogliono monitorare ciò che transita nella rete[57].

## ...collegati tra di loro

I grandi punti di interscambio sono collegati tra loro da grandi fasci di fibre ottiche. L'insieme di questi collegamenti formano le *dorsali* di internet (backbone)[58].
Per collegare l'Europa alle Americhe, diversi fasci di fibre ottiche corrono sul fondo dell'Oceano Atlantico. Questi fasci di fibre costituiscono altrettanti punti deboli, e di tanto in tanto capita qualche incidente, per esempio un'ancora di una nave che taglia un cavo rallenterà moltissimo internet in tutto un intero continente[59]. Può sembrare strano, considerando che storicamente l'idea di internet era di ispirazione militare: una rete decentralizzata, che moltiplica i suoi collegamenti per continuare ad esistere in caso ne venisse reciso uno.

---

57 Guillame Champeau, 2013, *Come la Germania spia le nostre comunicazioni* [rucofu.vado.li].

58 https://www.submarinecablemap.com/

59 Pierre Col, 2009, *Internet, ancore di barche e terremoti sottomarini* [tamofo.vado.li]; Cécile Dehesdin, 2013, *Tagli ai cavi sottomarini stanno rallentando internet in diversi Paesi* [dulate.vado.li].

## 1.4.3 Routing

Abbiamo visto[60] che i computer scambiano informazioni sotto forma di pacchetti.
Immaginiamoci ora due computer connessi a internet su reti diverse che desiderano scambiarsi un mucchio di informazioni.
Ad esempio, il pc di Alice che si trova in Francia, si connette a quello di Betty che sta in Venezuela.

*Routing*

Il computer di Alice accede a internet tramite il suo "scatolotto", che si trova sulla rete del suo provider (l'ISP).
Il computer di Betty fa parte della sua rete universitaria.
Il pacchetto inviato per il computer di Betty arriverà prima sulla rete dell'ISP di Alice e sarà trasmesso al router C del suo ISP, che funge da centro di smistamento. Il router legge l'indirizzo del computer di Betty sul pacchetto e deve decidere a chi passarlo per avvicinarlo alla sua destinazione. In che modo decide?
Ciascun router mantiene un elenco delle reti alle quali è connesso. Inoltre invia regolarmente l'aggiornamento di questo

60 Cap. 1.2.5

elenco agli altri router a quali è connesso, i suoi vicini, che fanno lo stesso. È grazie a queste liste che si è in grado di indirizzare i pacchetti ricevuti e trasmetterli a destinazione.
Il router ISP di Alice sa che può unirsi alla rete universitaria di Betty tramite quattro intermediari inviando il pacchetto al router D. Ma può anche inviarlo tramite due intermediari, passandolo al router E. Sceglierà quindi di inviare il pacchetto a E, che ha un percorso più diretto.
Il pacchetto arriva così a E – il router di un operatore di transito, un'organizzazione pagata dall'ISP di Alice per instradare i pacchetti – e farà lo stesso tipo di calcolo inviando il pacchetto a F. La rete di F include computer non solo in Europa, ma anche nelle Americhe collegati da un cavo transatlantico. F è di proprietà di una società, simile a quella che gestisce E, pagata dall'Università di Betty. F alla fine invia il pacchetto al router dell'Università, che lo invia al computer di Betty.
Uff, ecco il nostro pacchetto arrivato a destinazione.
Con questo sistema, ogni pacchetto di informazioni che attraversa internet passa attraverso diverse reti. Ogni volta, un router funge da centro di smistamento e lo invia a un router vicino. Alla fine ciascun pacchetto passa attraverso tanti computer diversi, che appartengono a varie e diverse organizzazioni.
Inoltre, la topologia della rete, cioè la sua architettura, la disposizione delle varie postazioni informatiche e la loro gerarchia cambiano nel tempo.
Quando Alice si connette di nuovo al computer di Betty il giorno successivo, i pacchetti inviati dal suo computer non seguiranno necessariamente lo stesso percorso del giorno prima. Ad esempio, se il router E è spento a causa di un'interruzione di corrente, il router dell'ISP di Alice instraderà il pacchetto attraverso D, che in precedenza rappresentava un percorso più lungo.
Agendo a livello di routing, il governo egiziano ha interrotto internet durante le rivolte del 2011. I router dei principali

ISP del paese hanno smesso di comunicare agli altri router a chi dovevano indirizzarsi per instradare i pacchetti destinati ai computer egiziani[61]. In questo modo i pacchetti destinati all'Egitto non riuscivano a trovare la strada e si è di fatto interrotto l'accesso a internet, il tutto senza tagliare neanche un cavo.

## 1.5 Sui client, sui server

Storicamente, negli anni 80, ogni computer connesso a internet forniva una parte di internet. Cioé non solo veniva usato per "andare a vedere cose su internet", ma offriva anche delle vere e proprie informazioni, dei dati e dei servizi ad altri utenti connessi. Un computer "faceva" internet e al tempo stesso ci accedeva.
Al giorno d'oggi il quadro generale è molto diverso. Abbiamo visto che ci sono computer costantemente accesi – i router – che sono responsabili del collegamento tra le varie parti di internet. Allo stesso modo, esiste un'altra categoria di computer sempre accesi che contengono quasi tutti i dati e i servizi disponibili. Questi computer vengono chiamati server, perché offrono informazioni e servizi centralizzando la maggior parte dei contenuti, che si tratti di siti web, musica, email, ecc. Questo porta a un certo tipo di verticalità nella gerarchia della rete. In effetti, in senso lato, più informazioni abbiamo, più potenzialmente potere abbiamo.
I server offrono, a differenza dei client che accedono solo alle informazioni. Questa situazione corrisponde a un internet in cui le nostre macchine svolgono principalmente il ruolo di clienti (client), centralizzando il potere attorno ai fornitori di

---

61 Stéphane Bortzmeyer, 2011, *Sospensione di internet in Egitto* [tosezo.vado.li].

contenuti[62]. Prendiamo l'esempio di uno dei servizi disponibili su internet, il sito web della Guida all'autodifesa digitale (`guide.boum.org` e `numerique.noblogs.org`): quando Alice visita una pagina di questo sito web, il suo computer funge da *client* collegandosi al *server* che ospita la Guida.
Nonostante ciò, qualsiasi computer può essere sia client che server, contemporaneamente o in successione. Questo è particolarmente vero con il modello peer-to-peer (P2P) ampiamente utilizzato nella condivisione di file. In questa situazione ciascun "nodo" è collegato alla rete e comunica svolgendo sia il ruolo di client che quello di server. I due ruoli non dipendono dalla macchina che usiamo.

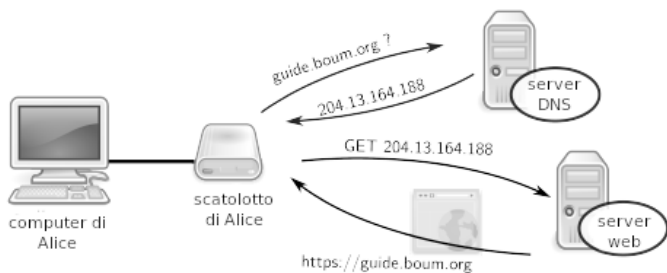
### 1.5.1 I DNS

Quando Alice chiede al suo browser web di accedere al sito della Guida, il suo computer deve connettersi al server che ospita questo sito.
Per fare ciò, è necessario conoscere l'indirizzo IP[63] del server. Tuttavia, un indirizzo IP è una serie di numeri che è abbastanza difficile da memorizzare, digitare o trasmettere: `204.13.164.188` (un indirizzo IPv4). Per risolvere questo problema, ci sono server a cui è possibile porre domande (qual è l'indirizzo IP di `guide.boum.org`?) come si cercherebbe nell'elenco telefonico il numero corrispondente. Questo sistema è chiamato DNS (Domain Name System). Il computer di Alice inizia quindi tramite il suo "scatolotto" a interrogare il DNS del suo ISP per ottenere l'indirizzo IP del server che ospita il dominio `guide.boum.org`.

62 La conferenza di Benjamin Bayart, *internet o Minitel 2.0* (conferenza all'8° World Free Software Meetings, 13 luglio 2007, Amiens) spiega molto bene questo cambiamento e le questioni a riguardo [moneva.vado.li].
63 Cap. 1.2.5

Il computer di Alice riceve in cambio l'indirizzo IP del server e possono quindi comunicare.

### 1.5.2 Percorso di una richiesta web

Il computer di Alice si connette quindi al server della Guida (204.13.164.188) e le invia una richiesta che significa "inviami la homepage del sito `guide.boum.org`". I pacchetti che trasportano la richiesta lasciano il suo computer, passano attraverso il suo "scatolotto" per raggiungere il router del suo ISP. Quindi, dopo aver attraversato diverse reti[64] e router[65] (non mostrati nel diagramma), può raggiungere il server di destinazione.

*Schema di un percorso di una richiesta web*

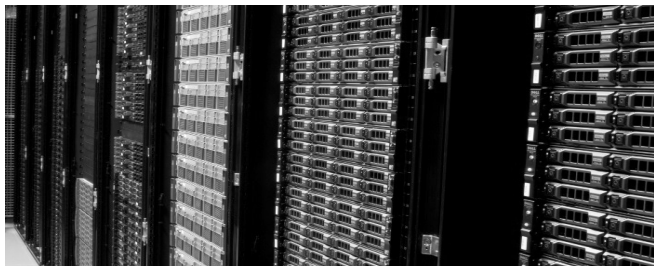
### 1.5.3 Server

Per inviare la pagina web richiesta da Alice, il server la cerca nella sua memoria, sul suo hard-disk, oppure la crea: non è detto che al momento della nostra richiesta le pagine esistano

64 Cap. 1.4.2
65 Cap. 2.3

già in una forma visualizzabile dal nostro computer. Spesso vengono generate automaticamente sul momento. In questi casi si parla di "web dinamico", contrapposto al "web statico" le cui pagine sono scritte in anticipo.
Ad esempio, se cerchiamo "ristorante tarapia tapioco" il motore di ricerca non ha ancora la risposta. Il server deve prima eseguire il codice sorgente[66] del sito in modo da calcolare la pagina contenente la risposta, e solo a quel punto ce la invierà. Su un server insomma è presente un software attivo che risponde quando gli viene fatta una richiesta. Questo tipo di software cambia a seconda dell'applicazione e fa parte di quel livello che include anche il protocollo applicativo[67]. Nel nostro esempio, quello che fa il software è cercare e offrire al computer di Alice la pagina web richiesta: questo tipo di programma si chiama "web server".

### 1.5.4 L'hosting dei server

I server sono generalmente raggruppati in edifici con una buona connessione alla rete e un'alimentazione elettrica molto affidabile: i "data center".

66 Tomo I, cap. 4
67 Cap. 1.2.3

Al giorno d'oggi, è di moda parlare di "cloud computing". Si tratta di un concetto di marketing che non mette in discussione la separazione tra client e server, anzi. Significa semplicemente che è possibile che i dati vengano spostati da un server a un altro, per motivi legali, tecnici o economici. E questo senza che i loro proprietari ne siano necessariamente informati.

*Ad esempio, Google dispone di almeno 15 data center distribuiti in 3 continenti*[68] *per garantire l'operatività dei suoi servizi 24 ore al giorno, 7 giorni alla settimana, anche quando alcune apparecchiature non sono disponibili.*
*Questo tipo di hosting mette insieme centinaia di macchine fisiche in diversi data center in tutto il mondo e somma la loro capacità di archiviazione e di elaborazione in modo da renderlo una "super macchina astratta". Successivamente rivende frazioni della potenza di calcolo e della memoria di questa super macchina, chiamandole "macchine virtuali". "Amazon Elastic Compute Cloud" o EC2 è uno dei servizi più conosciuti in questo campo*[69].

Una macchina virtuale può essere tranquillamente spostata in base all'utilizzo della macchina fisica, della qualità della connessione, della rete, ecc. Con un'infrastruttura del genere, è impossibile sapere in anticipo su quale macchina fisica o in quale posto si trovi esattamente una macchina virtuale.
Ciò rende praticamente impossibile avere il controllo sui nostri dati[70]. Verranno cancellati per davvero dalle macchine fisiche, quando pensiamo di "cancellarli"? Abbiamo visto nel primo volume che cancellare i dati su un computer non è affatto banale[71]. La questione si complica ulteriormente se non

68 Google, *Data center locations* [veredu.vado.li].
69 Wikipedia, *Amazon EC2.*
70 Jos Poortvliet, 2011, *openSUSE and ownCloud* [tudupa.vado.li].
71 Tomo I, cap. 4.3

sappiamo di quale computer si tratta. Inoltre, pone problemi legali: ad esempio dei dati detenuti legalmente possono diventare illegali se la macchina che li contiene cambia giurisdizione.
Insomma c'è stato un passaggio da un internet in cui tutti consultavano e al tempo stesso distribuivano dati, a un modello in cui i dati erano centralizzati su macchine fisiche chiamate server, arrivando ai giorni nostri con il cloud, dove i dati vengono salvati, a volte in modo casuale, su server non specificati. Alla fine, diventa estremamente complicato sapere dove sono effettivamente archiviati e l'utente ha sempre meno controllo sul loro destino.

# 2 | Tracce da tutte le parti

Il normale funzionamento delle reti prevede che si sappia che cosa avviene all'interno di molti computer. Non si tratta di sorveglianza attiva, a volte è completamente necessario per il loro funzionamento. Capita, ad esempio, che queste informazioni vengano raccolte perché "convenienti" per diagnosticare problemi. Tuttavia, il funzionamento di un qualsiasi computer lascia un certo numero di tracce, tema affrontato nel primo volume di questa Guida[1].
Nel caso dell'utilizzo online, non è solo il computer che hai davanti che può tenere traccia di ciò che fai in rete, ma anche ciascuno dei computer attraverso il quale transitano le informazioni, se esse circolano così come sono, vale a dire "in chiaro" e non crittografate[2].

## 2.1 Sul computer del client

Il client utilizzato per la rete ha accesso a tutto ciò che gli serve per connettersi. E come per ogni altro utilizzo, il computer spesso lascia tracce.
Come è stato ampiamente spiegato nel primo tomo, queste tracce e la facilità con cui possono essere utilizzate dipendono in gran parte dal computer e dal sistema operativo utilizzato.

### 2.1.1 La memoria del browser

Per essere più piacevole da usare, i browser web registrano molte informazioni sulle pagine che consultiamo. Alcuni

1 Tomo I, cap. 2
2 Tomo I, cap. 5.1

esempi: la maggior parte mantiene una cronologia delle pagine visualizzate; spesso si offrono di registrare ciò che l'utente inserisce nei moduli presenti su determinate pagine, nonché le password dei vari account; generalmente registrano le pagine recentemente o attualmente consultate, per accelerarne il caricamento: si parla di "caching"[3]. Questo è uno dei modi con cui un'autorità può monitorare la nostra navigazione su internet. Ricordiamoci l'inizio della nostra storia:

"*A quanto pare, sul computer utilizzato per caricare gli estratti conto, ci sarebbe stato un collegamento a una casella di posta in Gmail il cui indirizzo corrisponde a una certa Alice; così come un altro indirizzo di posta elettronica non loggato, poco prima della pubblicazione dei documenti offensivi*".

### 2.1.2 I cookie

Il termine cookie deriva dall'inglese "*fortune cookie*" in riferimento ai dolcetti che nascondono all'interno un messaggio scritto su un piccolo pezzo di carta. Un cookie è un piccolo "testo" inviato da un sito web che il browser dell'utente memorizza e rinvia ad ogni visita. Questo è ciò che consente, ad esempio, alle applicazioni di posta online (webmail) di ricordare che siamo autenticati con il nostro indirizzo e la nostra password durante la sessione internet, oppure di memorizzare la lingua che vogliamo usare.
I cookie consentono inoltre a un sito web di tenere traccia delle persone che lo visitano.
Le agenzie di pubblicità online includono negli annunci cookie di tracciamento, che consentono di seguire l'utente nei suoi

3 Per visualizzare il contenuto della cache del browser web Firefox o di uno dei suoi derivati, come Iceweasel o Tor Browser, digitare `about:cache` nella barra degli indirizzi.

movimenti su tutti i siti che visualizzano annunci della stessa agenzia. In questo modo possono "raccogliere informazioni sempre più precise e di conseguenza offrirgli una pubblicità sempre migliore e mirata"[4].
Infatti, quando si consultano alcune pagine web, sono esse stesse a collegarsi direttamente a siti pubblicitari aumentando ulteriormente le possibilità di tracciamento.
Infine, alcuni cookie hanno una data di scadenza, ma altri sono a durata indefinita: i siti che ce li hanno trasmessi saranno in grado di identificare il nostro browser per anni!
I cookie classici sono tuttavia limitati in termini di volume di dati e facili da eliminare, per un utente informato. Sono stati anche "migliorati" tramite la tecnologia Flash da un "local shared object" (LSO), detto anche "Flash cookie", che permette di immagazzinare più dati[5].
Il nuovo standard HTML5 include un meccanismo simile, chiamato "Archiviazione web locale"[6].
Altre tecniche consistono nel memorizzare lo stesso cookie in posizioni diverse nel browser e ricreare ad ogni visita quelli cancellati, partendo dal presupposto che sebbene ciascun cookie possa essere cancellato, non saranno cancellati tutti contemporaneamente[7].

### 2.1.3 Applicazioni lato client

Nell'evoluzione del web e dei suoi browser, da subito è stato chiaro che per avere un minimo di interattività era necessa-

4 CNIL, 2009, *La pubblicità online mirata*, M. Peyrat [viripu.vado.li].
5 Wikipedia, *Local shared object (LSO).*
6 Simon K., 2012, *Stockage des données locales: Web Storage* [cirite.vado.li].
7 La libreria JavaScript evercookie [https://samy.pl/evercookie/] è un esempio di questo tipo di tecnologia.

rio che parte del codice sorgente[8] del sito fosse eseguito lato client, dal browser, e non sul server[9] che lo ospita.
Ci sono anche diversi aspetti pratici: lato server web, significa meno lavoro e risparmio sull'hardware; lato client, la visualizzazione e le funzionalità del sito sono accelerate. Aiuta anche a ridurre al minimo il traffico di rete tra il browser e il sito: non è necessario richiedere una pagina completa ogni volta che si fa clic su un piccolo pulsante, ma basta trasmettere solo un piccolo frammento della pagina.
Sono state sviluppate delle tecnologie per abilitare queste funzioni: JavaScript e Ajax, Flash e Java sono le principali.
Queste funzionalità extra hanno però un "costo": significa che l'autore di un sito è in grado di eseguire il suo codice su tutti quei computer che lo visitano (il che pone molti problemi di sicurezza, come abbiamo visto nel primo tomo[10]). Ovviamente sono state messe in atto alcune protezioni all'interno dei browser[11], ma non coprono tutti i rischi e comunque non sostituiscono la vigilanza degli utenti di internet[12].
Queste tecnologie hanno funzionalità che, se da un lato possono essere utili, dall'altro sollevano alcuni interrogativi. Flash o WebRTC[13] possono accedere al microfono e alla fotocamera del computer su cui vengono eseguiti[14]. Nel caso di Flash, parliamo di un software proprietario[15] e il suo uso pone delle questioni, perché il tempo di esecuzione non può essere ispe-

8 Tomo I, cap. 4.1.1

9 Cap. 1.5.3

10 Tomo I, cap. 4.1.2

11 Generalmente implica solo dare accesso al codice dei siti web a funzioni limitate eseguendolo in una "sandbox" (Wikipedia, *Sandbox*).

12 Felix Aimé, 2012, *Sicurezza dei navigatori*.

13 Tecnologia che mira a integrare comunicazioni in tempo reale nei browser web, ad esempio Voice over IP (VOIP).

14 Una falla nella sicurezza di Flash ha consentito a qualcuno di attivare involontariamente le webcam delle persone che visitano un dato sito web.

15 Tomo I, cap. 4.1

zionato e le correzioni per le falle di sicurezza possono essere gestite solo dalla società Adobe che lo distribuisce.
Abbiamo visto che riporre la propria fiducia nel software[16] è una scelta complessa e l'esecuzione di questi programmi solleva interrogativi sul potere concesso agli autori di siti o applicazioni web, di accedere alle risorse del nostro computer e alle informazioni in esso contenute.
Inoltre, prima di essere eseguiti dal browser, questi pezzi di codice passano attraverso la rete, spesso senza alcuna autenticazione. Ciò lascia la discrezione alle persone se modificarli e come (per introdurre malware, ad esempio) così come il resto di una pagina web.
È anche possibile giocare con i dati che questi codici devono elaborare per cercare di deviarne l'utilizzo: un tipo di manipolazione di alcune pagine è accaduto, ad esempio, quando è stato utilizzato un punto di accesso wi-fi di un hotel di New York che utilizzava apparecchiature di rete dedicate a questo compito[17].
Alla fine, un browser web moderno ha così tante funzionalità che un potenziale avversario ha un numero considerevole di zone in cui sferrare un attacco.

## 2.2 Nella scatola: l'indirizzo fisico della scheda di rete

Abbiamo visto che la scheda di rete utilizzata da qualsiasi computer per connettersi ha un indirizzo hardware (MAC address[18]) che viene utilizzato dalle apparecchiature di rete per reindirizzare un pacchetto di dati alla scheda di rete corretta, ad esempio quando più computer sono collegati alla stessa

16 Tomo I, cap. 3
17 Justin Watt, 2012, H*otel Wifi JavaScript Injection* [zubima.vado.li].
18 Cap. 1.1.2

"scatola". Normalmente, questo indirizzo non esce dalla rete locale e di solito ci colleghiamo direttamente alla "scatola" di un provider di servizi internet.
Ogni scheda di rete connessa fornisce quindi il proprio indirizzo hardware e la maggior parte conserva un registro che contiene gli indirizzi, almeno finché sono attive. Non dovrebbero far trapelare questo diario, tuttavia è difficile conoscere i tipi e la quantità di informazioni contenute, comprese la potenziale esistenza di backdoor[19] o falle nella sicurezza. In effetti, queste "scatole" funzionano con il software[20] installato dal provider di servizi internet, che mantiene un accesso privilegiato, quantomeno nell'aggiornamento del software. Per noi la "scatola" è quindi da considerare come una vera e propria scatola nera, della quale dunque non abbiamo le chiavi, e che può sapere – e fare – molte cose sulla rete locale.

*Se ci piace smanettare, si può sostituire il firmware del router con un sistema operativo gratuito come LEDE[21]. Alcuni fornitori di accesso a internet associativi forniscono ai propri membri router che utilizzano solo software gratuito[22].*

Quando la rete locale prevede l'utilizzo del wi-fi è possibile che, più o meno accidentalmente, gli indirizzi hardware dei computer che si connettono alla scatola vengano registrati da altri computer "in ascolto". È così che Google Cars, mentre percorreva migliaia di strade per stabilire la mappa di Google Street View, ha colto l'occasione per "catturare" gli indirizzi MAC di alcuni computer con cui interagiva nel passaggio.
È possibile modificare temporaneamente l'indirizzo hardware

19 [sadeve.vado.li].
20 Tomo I, cap. 1.4
21 LEDE Project, 2017, *Reasons to use* LEDE [dagaci.vado.li].
22 Un elenco di modem e router utilizzati dai membri della Federazione FDN: Federazione FDN, 2017, *Modem e router* [zovofi.vado.li].

di una scheda di rete, ad esempio per non essere rintracciati con i nostri laptop[23] quando siamo in movimento.
È necessario citare i casi in cui si inserisce un login e una password nel proprio browser web per potersi connettere: è il caso delle reti wi-fi pubbliche, come quelle di un'area urbana, un'istituzione o un fornitore di accesso a internet (in Francia FreeWifi, SFR WiFi public e wi-fi Bouygues Telecom) che sono chiamati "captive portal". In questo caso, oltre all'indirizzo hardware della scheda wi-fi, viene fornito all'organizzazione che gestisce il portale l'identità dell'abbonato.

## 2.3 All'interno dei router: gli header dei pacchetti

Sulla strada tra un computer e il server a cui ci si vuole connettere, ci sono molti router[24], che ritrasmettono i pacchetti e li inviano al posto giusto.
Per sapere dove inviare un pacchetto, questi router leggono una sorta di busta su cui è scritta una certa quantità di informazioni; questa "busta" è chiamata "header" dei pacchetti.
L'header[25] contiene molte informazioni necessarie per il suo instradamento, compreso l'indirizzo IP del destinatario, ma anche quello del mittente (a cui deve essere inviata la risposta). Il router vede così quale computer vuole parlare con quale altro computer, così come il postino deve avere l'indirizzo del destinatario per trasmettergli la posta e l'indirizzo del mittente per un eventuale ritorno.
Contengono anche il numero di porta[26] di origine e il numero di porta di destinazione, che possono fornire informazioni sull'applicazione utilizzata.

---

23 Wikipedia, *Mac Spoofing.*
24 Cap. 1.4.2
25 Cap. 1.2.5
26 Cap. 1.2.6

Per svolgere il proprio lavoro, i router *devono* leggere queste informazioni; possono anche tenerne traccia sui log.
Sebbene non abbiano una buona ragione per farlo, i router sono anche in grado di accedere *all'interno* della busta trasportata; ad esempio, il contenuto della pagina web visualizzato da un utente internet[27] o quello di un'email inviata[28] (Deep Packet Inspection o DPI).
Ad esempio, il fornitore di servizi internet francese Orange include nei contratti dei suoi abbonati una clausola relativa all'uso dei "dati relativi" al suo traffico[29].

## 2.4 All'interno del server

Il server ha accesso, come i router, agli header dei pacchetti IP e quindi a tutte le informazioni di cui abbiamo appena parlato. In particolare, guarda l'indirizzo IP[30] della scatola utilizzato dal computer che si connette per sapere a chi inviare la risposta.
Oltre alle intestazioni IP, corrispondenti al livello di rete[31] della comunicazione, il server leggerà gli header del protocollo applicativo[32] che corrispondono al livello applicativo della comunicazione.
Ma il server legge anche il contenuto dei pacchetti stessi: è infatti il server che deve aprire la busta e leggere la lettera per rispondere. Il software del server interpreterà quindi la lettera ricevuta, scritta con il protocollo applicativo, per fornire la risposta appropriata.

27 Cap. 3.4.3
28 Wikipedia, *Deep Packet Inspection.*
29 [togila.vado.li].
30 Cap. 1.5.2
31 Cap. 1.2.2
32 Cap. 1.2.3

Tuttavia, molti protocolli applicativi trasmettono anche informazioni che identificano il computer che si sta connettendo.
I server, come i computer client, hanno registri di sistema: questo sarà discusso più approfonditamente nella sezione successiva[33].

### 2.4.1 Gli header HTTP

Quando un browser richiede una pagina web, include nella richiesta il nome del software, il suo numero di versione, il sistema operativo utilizzato e la lingua in cui è configurato. Ecco una richiesta inviata dal browser web Firefox:

```
GET /index.html HTTP / 1.1
Host: example.org
User-Agent: Mozilla / 5.0 (X11; Linux x86_64; rv: 52.0)
Gecko / 20100101 Firefox / 52.0
: testo / html, application / xhtml + xml, application /
xml; q = 0.9, * / *; q = 0,8
Accept-Language: fr-FR, en; q = 0,5
Accept-Encoding: gzip, deflate
Referer: www.google.com/search?q=example+domain&... oe =
utf-8 & aq = t
Cookie: PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120
```

Vediamo prima un comando contenente il nome della pagina richiesta (`index.html`), il nome di dominio corrispondente (`www.example.org`), seguito da un'intestazione che contiene tra l'altro il nome e la versione del browser (`Mozilla / 5.0 Gecko / 20100101 Firefox / 52.0`) nonché il sistema operativo utilizzato (`Linux x86_64`), le lingue accettate (`fr-FR` per il francese

33 Cap. 3

della Francia, `en` per l'inglese), la pagina in cui si trovava il collegamento che l'utente internet ha seguito per raggiungere la pagina richiesta (www.google.com/search?q=example+domain&..., nota i termini di ricerca: "example" e "domain") e il cookie[34] di sessione (`PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120`). Queste informazioni servono per essere utilizzate dal server web, che adatterà la sua risposta in funzione alla richiesta: grazie a questo, un sito disponibile in più lingue sarà visualizzato nella nostra senza che lo dobbiamo continuamente indicare.
Ma queste informazioni, come tutte quelle che passano attraverso il server, sono accessibili anche alle persone che si occupano della manutenzione: i suoi amministratori e i loro capi. In generale, i server conservano anche queste informazioni nei log[35], per un tempo più o meno lungo, in particolare per fare statistiche e per facilitare la diagnostica in caso di guasto. Aggiungono l'indirizzo IP originale insieme alla data e all'ora alle intestazioni. Ecco un esempio per la nostra query (l'indirizzo IP è all'inizio: `203.0.113.16`):

```
203.0.113.16 – - Jan “GET /page.html HTTP / 1.1” 200
9042 “http://www.example.org/index.html” “Mozilla / 5.0
(Windows; U; Windows NT 6.1; en-US; rv: 1.9.2.3) Gecko /
20100401 Firefox / 3.6.3 “
```

### 2.4.2 Gli header delle email

Ogni email include un'intestazione; nonostante il nome, non ha a che fare con gli header di una pagina web che contengono informazioni sui dati nell'email: un altro esempio di metadati,

34 Cap. 2.1.2
35 Cap. 3.2.2

"dati sui dati"[36]. Raramente sono mostrati nella sua interezza dal nostro software di posta elettronica, ma sono comunque presenti. Spesso includono molte informazioni sul mittente, molto di più del solo indirizzo email.
Nell'esempio seguente possiamo leggere l'indirizzo IP pubblico, ovvero quello che sarà visibile su internet[37], del computer utilizzato per inviare l'email (`203.0.113.98`), che permette di conoscere la posizione in cui il mittente era in quel momento, l'indirizzo IP del suo computer all'interno della sua rete locale (`192.168.0.10`), il software di posta elettronica utilizzato (Thunderbird / 45.8.0) e il sistema operativo (OS X):

```
Return-Path:
Delivered-To: alice@exemple.org
Received: from smtp.fai.net (smtp.fai.net 198.51.100.67)
by mail.exemple.org (Postfix) with ESMTP id 0123456789
for ; Sat, 1 Jan 2014 20:00:00 +0100 (CET)
Received: from 192.168.0.10 (paris.abo.fai.net
203.0.113.98)
by smtp.fai.com (Postfix) with ESMTP id ABCDEF1234;
Sat, 1 Jan 2014 19:59:49 +0100 (CET)
Message-ID:
Date: Sat, 1 Jan 2014 19:59:45 +0100
From: Betty
User-Agent: User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
OS X 10.12; rv:45.0)
Gecko/20100101 Thunderbird/45.8.0
MIME-Version: 1.0
To: Alice
Subject: À mardi
Content-Type: text/plain; charset=iso-8859-1
```

36 Tomo I, cap. 2.6
37 Cap. 1.3.4

```
Content-Length: 22536
Lines: 543
```

Queste intestazioni a volte contengono anche l'identificativo dell'abbonato con il suo provider di posta elettronica o il nome della sua macchina[38].
Sono bastati pochi esempi comuni per comprendere che quasi tutte le applicazioni inviano informazioni sul contenuto, ma anche metadati[39] nel loro protocollo.

## 2.5 Le tracce che lasciamo da soli

Non ci sono solo le tracce che lascia il funzionamento delle reti, ma ovviamente anche quelle che lasciamo volontariamente o meno, ad esempio inserendo informazioni sui siti web o semplicemente connettendoci ai servizi.
Cercare di controllare le tracce che lasciamo in rete significa quindi pensare anche agli usi che facciamo dei servizi offerti e ai dati che gli affidiamo – temi che tratteremo più avanti.

38 Il più delle volte si trova nella riga `Received` o nel `Message-Id`, ma alcuni software o servizi di messaggistica aggiungono altre linee più specifiche.
39 Tomo I, cap. 2.6

# 3 | Sorveglianza e controllo delle comunicazioni

Oltre alle tracce lasciate dal funzionamento generale della rete, è possibile “ascoltare” le nostre attività a più livelli: sempre più spesso le organizzazioni che fanno funzionare internet sono obbligate, dal punto di vista legale, a conservare un certo numero di informazioni riguardo a quello che succede sulle loro macchine, in nome della legge sulla Data Retention.

## 3.1 Chi vuole recuperare i dati?

Ci sono diverse persone o organizzazioni che possono voler posare lo sguardo sugli scambi che avvengono via internet. Genitori troppo curiosi, siti web alla ricerca di consumatori da profilare, multinazionali come Microsoft, la polizia, o la NSA americana... Come già abbiamo visto nel caso dei malware[1], le differenti entità implicate generalmente non collaborano tra di loro, né formano un’unica totalità coerente. I curiosi sono troppi per pretendere di fare una lista esaustiva degli interessi in gioco, possiamo però descrivere qualcuna delle motivazioni più ricorrenti.

### 3.1.1 Aziende alla ricerca di profili da rivendere

“Decidete di prenotare un biglietto d’aereo per New York su internet. Due giorni dopo, leggendo il vostro quotidiano online, una pubblicità vi propone un’offerta interessante per un noleggio di automobili a New York. Non si tratta solo di una semplice coincidenza: è un meccanismo di pubblicità mirata,

1 Tomo I, cap. 3

come ormai se ne sviluppa sempre di più su internet"[2].
La pubblicità è una delle principali fonti di reddito per le aziende che forniscono servizi "gratuiti": caselle di posta, motori di ricerca, social media, ecc. Dal punto di vista degli inserzionisti, tuttavia, la qualità e quindi il costo di uno spazio pubblicitario online dipendono dall'interesse che gli utenti dimostrano per gli annunci.
Quindi, i dati personali valgono oro. Interessi, sesso, età, tante informazioni che consentono di proporre inserti a cui è probabile che l'utente reagisca. Ad esempio, Gmail – il servizio di posta elettronica di Google – utilizza il risultato dell'analisi del contenuto delle email per visualizzare offerte pubblicitarie corrispondenti[3]: per fare un esempio (autentico! ), una persona in procinto di separarsi dal partner potrebbe visualizzare, accanto alle sue email, annunci di siti di incontri...
Inoltre, ogni sito visitato è un "centro di interesse". Sommando queste informazioni insieme, emerge un intero profilo[4]. Esiste un piccolo software che permette di vedere quali cookie[5] sono stati scaricati sul nostro computer per ogni pagina consultata[6]. Ad esempio, se l'utente inizia la navigazione consultando allocine.fr, quattro agenzie pubblicitarie registreranno la sua visita. Andando a leggere poi le ultime notizie su "Le Monde", altre quattro agenzie verranno coinvolte, due delle quali già presenti sul primo sito visitato. Si saprà, quindi, che l'utente ha interagito con queste due pagine e ora potranno essere abbinate come "centro di interesse". Proseguendo suc-

---

2 CNIL, 2009, *La pubblicità mirata in rete* [nirave.vado.li].

3 "Elaboriamo automaticamente i tuoi messaggi per aiutarti a ordinarli. [...] Lo stesso vale per gli annunci. [...] Il processo di visualizzazione degli annunci in Gmail è completamente automatizzato. Nessuno legge le tue email al fine di scegliere gli annunci che vi saranno presentati". Google, 2017, *Come funzionano gli annunci in Gmail.*

4 Data Gueule, 2014, *Big data: données, données, donnez-moi!* [litili.vado.li].

5 Cap. 2.1.2

6 Mozilla, *Lightbeam add-ons per Firefox.*

cessivamente su Gmail e Dailymotion, un totale di 21 agenzie pubblicitarie sarà a conoscenza dell'accesso.
In ciascuna di queste sessioni, troveremo come riferimento agenzie pubblicitarie come XiTi e Google-Analytics. Il più grande motore di ricerca è a conoscenza dei siti visitati e può quindi impostare una pubblicità mirata.
I social media sono particolarmente adatti per ottenere direttamente dagli utenti i dati personali che li riguardano. Ad esempio, un inserzionista su Facebook può "indirizzare un annuncio pubblicitario a persone di età compresa tra i 13 e i 15 anni, che vivono a Birmingham in Inghilterra e che hanno il "bere" come centro di interesse. Facebook indica che il target scelto comprende circa un centinaio di persone[7], dimostrando di sfruttare i dati che raccoglie dai propri membri per fornire una pubblicità altamente mirata"[8].
La pubblicità mirata è uno dei motivi che hanno spinto gli operatori a diversificare i propri servizi e le proprie attività, al fine di raccogliere sempre più informazioni sul comportamento degli utenti. Ad esempio, Google che come sappiamo fornisce servizi di ricerca, ha rilevato società pubblicitarie come DoubleClick. Recentemente ha lanciato un servizio, Google Suggest, integrato nel suo browser Chrome che gli invia tutte le pagine web visitate, anche quando non sono state visualizzate tramite il motore di ricerca[9]. Per dare un'idea dell'importanza della posta in gioco, ricordiamo che Google ha acquisito la Doubleclick per 3,1 miliardi di dollari[10].
L'accumulo di dati e la loro elaborazione gli consente inoltre di ordinare e adattare i risultati ai presunti centri di interesse

7 Un'interfaccia simile è pubblicamente disponibile e permette di rispondere a richieste un po' inquietanti. Ne parla Tom Scott in *Actual Facebook Graph Searches*, 2014 [tesudi.vado.li].

8 CNIL, 2009 La pubblicità mirata in rete (in francese), op. cit., p. 13.

9 CNIL, 2009 La pubblicità mirata in rete (in francese), op. cit., p. 4.

10 Le Monde, 2007, *Google rachète DoubleClick pour 3,1 milliards de dollars* [debofo.vado.li].

degli utenti. Quindi, data un'identica ricerca, due persone con profili diversi non otterranno lo stesso risultato, il che ha come riflesso quello di rafforzare i propri interessi e le convinzioni di ciascuno. È ciò che alcuni chiamano "filter bubble"[11].

Oltre che per temi, la pubblicità è anche mirata anche geograficamente: grazie al GPS integrato nei dispositivi mobili come gli smartphone, ma anche grazie all'indirizzo IP e alle reti wi-fi "visibili" alla portata del laptop o del telefono[12]. In questo modo, ad esempio, è possibile far visualizzare annunci riferiti a negozi che si trovano nei pressi dell'abbonato.

Gli interessi economici spingono quindi i fornitori di servizi a raccogliere i profili degli utenti nel modo più preciso possibile, per poi vendere direttamente o indirettamente spazi pubblicitari mirati.

Le aziende in questione, una volta raccolte queste informazioni, generalmente non saranno riluttanti a condividerle con dei poliziotti, se glielo chiedono. Tutti i grandi fornitori di contenuti hanno uffici dedicati a rispondere alle domande e dunque hanno elaborato moduli e procedure per comunicare con i poliziotti, spiegandogli la via migliore per richiedere informazioni[13].

### 3.1.2 Aziende e Stati che cercano di preservare i propri interessi

Altre aziende sono interessate a ciò che accade su internet per proteggere i propri interessi. Stiamo parlando, ad esempio, della lotta condotta dall'industria dell'audiovisivo contro il

---

11 Xavier de la Porte, 2011, *Le risque de l'individualisation de l'internet* [numopa.vado.li].

12 Audenard, 2013, *Bornes wifi et smartphones dans les magasins, blogs/sécurité, Orange Business* [gusade.vado.li].

13 Negli ultimi anni sono trapelate diverse versioni di una guida pubblicata da Facebook [sodovu.vado.li]. Ne esistono anche altre della stessa risma (ma non è nemmeno tutto corretto) su cryptome.org [tegoma.vado.li].

download illegale o della tecnologia di sorveglianza: le imprese osservano e analizzano in tempo reale e in modo automatizzato centinaia di fonti (siti di notizie, deposito di brevetti, blog di esperti...) per conoscere rapidamente i più recenti progressi tecnologici ed essere più competitive.

Le imprese non sono certo le uniche a guardare con molto interesse internet: gli Stati, passando dalla giustizia ai servizi segreti, ai vari servizi di polizia, sono sicuramente i più curiosi. Sempre più Paesi stanno introducendo una legislazione che permetta di identificare gli autori a partire da tutte le informazioni che circolano su internet[14].

Ma siamo andati sicuramente oltre: le agenzie e altri servizi segreti non si accontentano più di spiare soltanto alcuni che considerano obiettivi da sorvegliare. Ai limiti della legalità, l'NSA – un'agenzia di intelligence statunitense – raccoglie "tutti i tipi di dati sulle persone – pensiamo che si tratti di milioni di utenti"[15]. Tra i suoi obiettivi: "esaminare" quasi tutto ciò che una persona fa su internet[16] e stabilire un grafico sociale, cioè "la rete di connessioni e relazioni tra individui"[17]. "Di solito, analizzano reti che sono a due gradi di distanza dall'obiettivo". In altre parole: l'NSA sta spiando anche chi comunica con chi viene spiato[18].

I servizi segreti francesi dispongono ora di un arsenale di leggi che gli consente di effettuare analisi di tutto il traffico o di persone mirate in tutta legalità, sia in Francia che all'estero[19].

---

14 Begeeek, 2013, *Facebook publie son premier rapport international des demandes gouvernementales* [bocera.vado.li].

15 Bruce Schneier, citato da Guillaud, 2013, *Lutter contre la surveillance: armer les contre-pouvoirs*, Internet Actu [dutata.vado.li]

16 Maxime Vaudano, 2013, *Plongée dans la «pieuvre» de la cybersurveillance de la NSA*, LeMonde.fr [damilo.vado.li].

17 Francis Pisani, 2007, *Facebook/5: la recette*, Transnets [nigeli.vado.li].

18 Manach, 2013, *Pourquoi la NSA espionne aussi votre papa* [ranite.vado.li].

19 République française, *Code de la sécurité intérieure*, articoli L851-2, L851-3 e L854-1.

## 3.2 Log e data retention

La maggior parte delle organizzazioni che forniscono servizi su internet (connettività, hosting di siti, ecc.) conservano in modo più o meno significativo tracce di ciò che gli capita tra le mani, nella forma di una sorta di diario di bordo delle connessioni: chi ha fatto cosa e quando. Questi registri si chiamano "log"[20].
Storicamente i log rispondono a una necessità tecnica: vengono utilizzati dalle persone che si occupano della manutenzione dei server, per diagnosticare e risolvere eventuali problemi. Tuttavia possono anche essere molto utili per raccogliere dati riguardo chi utilizza questi server.

### 3.2.1 Leggi sulla Data Retention

Da tempo, all'interno della maggior parte dei Paesi occidentali, i fornitori di servizi internet sono legalmente obbligati a conservare i propri log per un determinato periodo di tempo, in modo da poter rispondere a eventuali richieste legali. Le leggi che regolamentano la conservazione dei dati definiscono in modo più o meno chiaro quali informazioni devono essere conservate all'interno di questi registri. Anche il concetto di fornitore di servizio internet può essere inteso in modo piuttosto largo: un internet point per esempio è un fornitore del servizio internet, ma fornisce *anche* un computer per accedere alla rete.
Al di là degli obblighi legali, è probabile che molti fornitori di servizi internet conservino più o meno vaste quantità di informazioni sui propri utenti, soprattutto per scopi pubblicitari. Come abbiamo visto in precedenza, alcune aziende come Google, Yahoo o Facebook, sono particolarmente note

20 Tomo I, cap. 2.4

per avere questa abitudine. Ma essendo un dato di fatto che questo "modello di fornitura di servizi intrecciato con la pubblicità è quasi diventato la norma"[21], possiamo supporre che moltissime altre aziende facciano la stessa cosa anche se più discretamente.
Nel Regno Unito per esempio, un ISP ha fatto parlare di sé quando è venuto fuori che conservava le tracce di tutte le pagine web visitate dai propri utenti per sperimentare una tecnica di profilazione destinata a "offrire" della "pubblicità comportamentale"[22] [23].
Il server che ospita il contenuto che utilizziamo (un sito, una casella email..) e il fornitore di accesso a internet sono in una posizione strategicamente ottima, che gli permette di disporre delle informazioni utili a identificare chi sta effettuando la richiesta. In Francia sono questi soggetti in particolare ad essere sottoposti alle leggi sulla Data Retention.

### 3.2.2 I log conservati dai fornitori di hosting

Abbiamo visto che il server che ospita un servizio (un sito web, una casella mail, una chat, ecc.) ha accesso a una grande quantità di dati[24].
In Francia, la Legge per la Riservatezza nell'Economia Digitale (Loi pour la Confiance dans l'Économie Numérique)[25] (uscita in seguito alla direttiva europea 2006/24/EC sulla

---

21 CNIL, *La publicité ciblée en ligne* (op. cit.), p. 4.
22 CNIL, *La publicité ciblée en ligne* (op. cit.), p. 17.
23 Arnaud Devillard, 2009, *Affaire Phorm: Bruxelles demande des comptes au Royaume-Uni* [favaze.vado.li].
24 Cap. 2.4
25 République française, 2014, *Loi n. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, Journal Officiel n. 143 du 22 juin 2004 page 11168, NOR : ECOX0200175L.

Data Retention[26]) obbliga chi ospita contenuti pubblici a conservare "i dati utili a permettere l'identificazione" di "tutte le persone che hanno contribuito alla creazione di un contenuto messo online"[27]: scrivere su un blog o su un sito di informazione partecipata, inviare una mail, scrivere dentro una mailing-list, per esempio[28]. Nel concreto si tratta di conservare per un periodo di un anno gli eventuali identificativi o pseudonimi forniti dall'autore, ma più che altro l'indirizzo IP[29] associato a ciascuna modifica del contenuto. Si passa poi a fare una richiesta al provider della connessione internet che ha fornito quell'IP, e in questo modo generalmente si riesce a risalire fino al proprietario della connessione.
Inoltre, la legge relativa allo sviluppo in ambito militare[30], promulgata a fine dicembre 2013, permette di richiedere queste informazioni in tempo reale, con motivazioni piuttosto variegate: attacchi terroristici, cyber-attacchi, attentati a obiettivi strategici scientifici e tecnici, criminalità organizzata, ecc.
È dunque quest'obbligo alla conservazione dei dati che permette alla polizia, nella nostra storiella introduttiva, di ottenere informazioni dai fornitori di servizi che ospitano le caselle di posta incriminate:

---

26 EUR-lex, 2006, *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.*

27 République française, 2011, *Décret n. 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.*

28 Questo secondo la famigerata legge francese. La legge italiana, invece, obbliga soltanto i provider e non genericamente chi ospita i contenuti. Motivo per cui i servizi autogestiti in Italia hanno meno obblighi rispetto a quelli francesi [NdT].

29 Cap. 1.2.5

30 Legifrance, 2014, *loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.*

*Piuttosto che a no-log, andranno a chiedere a Gmail le informazioni su questi indirizzi mail. Una volta ottenuti, sapranno sicuramente mettere le mani sulle persone responsabili della pubblicazione.*

I fornitori di servizi potranno essere più o meno cooperativi riguardo al verificare che la richiesta che gli arriva dalle forze dell'ordine sia legale e riguardo al come rispondere: sembrerebbe che alcuni rispondano immediatamente a una semplice email delle guardie, mentre altri aspettino invece di ricevere un atto firmato da un giudice[31], o addirittura non rispondano alle richieste[32].
Non sono solo le persone che hanno accesso al server a poter collaborare con le guardie come par loro, ma anche un avversario potrebbe, nel caso di un computer personale, introdursi e spiare tutto quello che transita utilizzando delle falle, senza passare per una richiesta legale. In quel caso avrebbe allora accesso a tutti i dati conservati su quel computer, compresi i log.
Ma il server non conosce sempre l'identità reale dei client che gli si collegano: in genere tutto quello che può offrire è un indirizzo IP.
È qui che interviene il provider della connessione internet.

### 3.2.3 I log conservati dai provider internet (ISP)

Come abbiamo visto, accediamo a internet attraverso la mediazione di un fornitore di accesso a internet (ISP)[33]. Questo ISP in genere è un'azienda che fornisce uno "scatolotto" connesso a internet. Ma potrebbe trattarsi invece di un'as-

31 Globenet, 2014, *No-log, les logs et la loi* [cutate.vado.li].
32 Anonimo, 2010, *Analyse d'un dossier d'instruction antiterroriste* [detabu.vado.li].
33 Cap. 1.4.1

sociazione o di un'istituzione pubblica (una università, per esempio, quando utilizziamo le loro sale studio). Gli ISP sono anch'essi sottoposti alle leggi sulla Data Retention.
All'interno dell'Unione Europea esiste una direttiva che obbliga gli ISP a conservare le tracce di chi si connette, quando e da dove. In pratica consiste nel registrare quale indirizzo IP è stato assegnato a quell'abbonato in un determinato periodo. Lo stesso vale per le istituzioni che forniscono accesso a internet, per esempio le biblioteche e le università: in genere si è obbligati a connettersi tramite un nome utente e una password. In questo modo si può sapere chi utilizzava quella postazione in quel momento. La direttiva europea precisa che questi dati devono essere conservati da 6 mesi a 2 anni. In Francia la durata legale è di un anno[34].
Inoltre gli ISP e i servizi di hosting francesi sono tenuti a conservare le "informazioni fornite dall'utente al momento della sottoscrizione di un contratto o della creazione di un account" per un anno dopo la chiusura dell'account. "Nel caso in cui la sottoscrizione del contratto o dell'account avvenga dietro pagamento", devono conservare anche le informazioni relative al pagamento[35].
L'obiettivo delle leggi sulla Data Retention è insomma rendere facile, per le autorità, l'associazione di un nome a tutte le azioni che effettua su internet.
Per esempio, delle guardie che stanno indagando su un articolo pubblicato su un blog, possono chiedere ai responsabili del servizio che ospita il blog l'indirizzo IP della persona che ha pubblicato l'articolo, insieme alla data e l'ora corrisponden-

34 Parlement Européen et Conseil, 2006, *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.*

35 *Décret n. 2011-219 du 25 février 2011*, op. cit.

te. Una volta ottenute queste informazioni, vanno a chiedere all'ISP responsabile di quell'indirizzo IP, a chi era assegnato quell'IP al momento dei fatti.

*«Che storia! Ma che c'entra con il nostro ufficio?»*
*«Beh è proprio per questo che la chiamo. Dicono che hanno le prove che quei documenti siano stati pubblicati dal vostro ufficio. Gli ho detto che non sono stato io, che non so di cosa stanno parlando.»*

È esattamente di questo che si tratta quando, nella nostra storia iniziale, la polizia insiste, prove alla mano, che gli estratti conto sono stati pubblicati dall'ufficio di via Jaurès. Per prima cosa ha ottenuto dai fornitori dell'hosting del sito l'indirizzo IP che corrisponde alla connessione responsabile della pubblicazione dei documenti incriminati. Questo primo passo ha permesso di sapere da dove, da quale "scatolotto", proviene la connessione. La successiva richiesta all'ISP gli permette di risalire al nome dell'abbonato – in primis all'indirizzo – associato all'indirizzo IP.

### 3.2.4 Richieste legali

In Francia, quando le forze dell'ordine vogliono accedere ai log richiesti dalla legge sulla Data Retention, è previsto che passino per una *richiesta legale*: una richiesta ufficiale che obbliga le persone che amministrano un server a fornirgli le informazioni richieste... o a disobbedire. Queste richieste legali dovrebbero precisare di quali informazioni si tratta. Ma questo non viene fatto sempre, e i fornitori di servizi internet a volte danno più informazioni di quelle che gli richiederebbe la legge. Ecco l'estratto di una richiesta legale ricevuta da un servizio di hosting email francese, abbiamo reso anonima la casella di

posta in questione sostituendola con un generico “indirizzo”. L’ortografia non è stata modificata.

> **RICHIESTA GIUDIZIARIA**
> Ufficiale di Polizia In servizio alla B.R.D.P
> *Preghiamo e, nel caso, richiediamo:*
> Il **Signor presidente dell’associazione GLOBENET**, 21ter, rue Voltaire 75011 Paris
> *che abbia la cortesia di:*
> Riguardo l’indirizzo di posta indirizzo@no-log.org
> - Comunicarci **l’identità completa** (nome, cognome data di nascita, parentela) e le **coordinate** (postali, telefoniche, elettroniche e bancarie) del suo **titolare**
> - Indicarci i TRENTA ultimi dati di accesso (indirizzo IP, data ora e fuso orario) utilizzati per **consultare, scaricare o inviare messaggi** con il suddetto indirizzo (POP, IMAP o webmail)
> - Indicarci **se è attiva una redirezione** su questo indirizzo di posta ed eventualmente comunicarci la/le email di destinazione
> - Comunicarci il **numero di telefono** collegato all’abbonamento internet dell’account no-log.org “indirizzo” e i suoi **30 ultimi dati di accesso**
> - Comunicarci i TRENTA **ultimi dati di accesso** (indirizzo IP, data ora e fuso orario) alle **pagine di amministrazione** dell’account no-log “indirizzo”

Inoltre, è provato che le guardie talvolta richiedano queste informazioni attraverso una semplice email, ed è probabile che molti fornitori di servizi internet rispondano direttamente a queste richieste non ufficiali, ciò implica che *chiunque* potrebbe ottenere queste informazioni fingendosi della polizia.
Le richieste legali sono moneta corrente. I grandi fornitori di servizi internet ormai hanno dei servizi legali dedicati per ri-

spondere a queste, con tariffe diversificate per ciascun tipo di richiesta[36]. Dall'ottobre 2013, in Francia, si sono rese omogenee le tariffe di queste differenti prestazioni attraverso un tariffario indicizzato dallo Stato: per esempio identificare un abbonato a partire dal suo indirizzo IP costava 4€ (tariffa in vigore nell'ottobre 2013). Oltre le 20 richieste, la tariffa scendeva a 18 centesimi.
Durante la prima metà del 2016, Google ha ricevuto in media ogni mese 717 richieste di dati sui propri utenti da parte della Francia, per un totale di 5185 account – cifra in aumento costante dal 2009. Dopo un'analisi della correttezza delle richieste sul piano giuridico, la società ha risposto al 60% di queste[37]: l'altra metà delle richieste quindi non rientrava nel quadro di ciò che l'azienda riteneva essere legalmente obbligata a fornire.

## 3.3 Ascolto di massa

Oltre ai registri e alle richieste legali previste dalle leggi sulla conservazione dei dati, le comunicazioni via internet sono sistematicamente monitorate da vari servizi statali.
Un ex dipendente dell'AT&T – operatore di telecomunicazioni statunitense – ha testimoniato[38] che la NSA ha monitorato tutte le comunicazioni via internet e le conversazioni telefoniche che passavano attraverso un particolare impianto della stessa AT&T a San Francisco. È stato possibile grazie ad un supercomputer appositamente progettato per il monitoraggio

---

36 Christopher Soghoian, 2010, *Your ISP and the Government: Best Friends Forever* [mipaga.vado.li].
37 Google, 2017, *France - Google Transparence des informations* [vopolu.vado.li].
38 Mark Klein, 2004, *AT&T's Implementation of NSA Spying on American Citizens* [cidopi.vado.li].

di massa in tempo reale delle comunicazioni[39]. Inoltre, l'operatore ha affermato che strutture come quella sono probabilmente già presenti in altre città degli Stati Uniti, confermando le rivelazioni di un altro ex dipendente della NSA e della CIA[40]. I Servizi Segreti britannici avrebbero allestito strutture simili su più di 200 fibre ottiche sottomarine[41].
I servizi di sicurezza francesi sono ormai autorizzati a installare tali strumenti di analisi del traffico nella rete dei fornitori di servizi per «monitorare connessioni che possono rivelare una minaccia terroristica»[42].
La NSA ha inoltre ottenuto l'accesso diretto ai server di diversi giganti della rete (Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL e Apple)[43], permettendogli di accedere a dati che ospitano o che transitano sui loro server[44].
La DGSE, l'equivalente francese della NSA, dispone di un accesso diretto alle reti di Orange[45].
Allo stesso modo, le comunicazioni via satellite sono ascoltate dalla rete Echelon, un «sistema globale di intercettazione delle comunicazioni»[46] sviluppato dai Paesi anglosassoni[47]. Le in-

39 Reflets.info, 2011, *#OpSyria: BlueCoat maître artisan de la censure syrienne* [zadera.vado.li].

40 Craig Timberg et Barton Gellman, 2013, *NSA paying U.S. companies for access to communications networks* [sizepi.vado.li].

41 L'expansion.com, 2013, *"Operation Tempora": comment les Britanniques dépassent les Américains pour espionner internet* [fubago.vado.li].

42 République française, Code de la sécurité intérieure, article L851-3.

43 NSA, 2013, *Dates When PRISM Collection Began For Each Provider* [daciza.vado.li].

44 Le Monde, 2013, *Le FBI aurait accès aux serveurs de Google, Facebook, Microsoft, Yahoo! et d'autres géants d'internet* [dizubo.vado.li].

45 Jacques Follorou, 2015, *Espionnage: comment Orange et les services secrets coopèrent*, Le Monde [midilu.vado.li].

46 Wikipedia, *Echelon.*

47 Gerhard Schmid, 2001, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)* [zelani.vado.li].

formazioni riguardo questo sistema rimangono tuttavia poco chiare; la Francia, ad esempio, sembra gestire una rete per l'ascolto delle telecomunicazioni sul suo territorio[48].
La NSA controlla e verifica anche gli scambi di email al fine di stabilire una mappa delle relazioni tra tutti gli abitanti degli Stati Uniti[49]. Possiamo immaginare dunque che se anche tali "pratiche di ascolto" non sono ancora state segnalate in altre parti del mondo, è verosimile che siano ampiamente diffuse.
In più, soprattutto per chi gestisce nodi significativi della rete, l'uso ufficiale o meno della Deep Packet Inspection[50] (DPI) si sta diffondendo sempre più. Il vantaggio di questa tecnica rispetto a quelle più tradizionali è che il monitoraggio non si limita alle informazioni scritte nelle intestazioni[51] dei pacchetti IP, ma arriva al contenuto delle comunicazioni. Se queste non sono cifrate, ad esempio, è possibile trovare il contenuto completo delle email o l'insieme delle consultazioni e delle ricerche sul web.
L'utilizzo di questa tecnica, in Libia o in Siria, ad esempio, ha permesso di mettere inizialmente sotto sorveglianza digitale l'intera popolazione del Paese, per poi effettuare attacchi mirati[52]. La società francese Amesys, con l'aiuto e il sostegno del governo[53] dell'epoca, ha installato tali sistemi in Libia[54], Marocco, Qatar e Francia[55].

---

48 Wikipedia, *Frenchelon.*

49 Gorman, Siobhan, 2008, *NSA's Domestic Spying Grows As Agency Sweeps Up Data: Terror Fight Blurs Line Over Domain ; Tracking Email* [vegiri.vado.li].

50 Cap. 2.3

51 Cap. 2.3

52 Cap. 3.4

53 kitetoa, 2011, *Amesys: le gouvernement (schizophrène) français a validé l'exportation vers la Libye de matériel d'écoute massive des individus*, Reflets.info [favuro.vado.li].

54 Fabrice Epelboin, 2011, *Kadhafi espionnait sa population avec l'aide de la France* [nonobi.vado.li].

55 Jean Marc Manach, 2011, *Amesys surveille aussi la France* [lofitu.vado.li].

## 3.4 Attacchi mirati

Quando un utente o una risorsa disponibile in internet, come un sito web o una casella di posta elettronica, suscitano la curiosità di un qualche avversario, è bene tenere a mente che quest'ultimo può organizzare attacchi mirati su diversi livelli: le directory dove si trova la risorsa, i server che la ospitano, i client che vi accedono, ecc. In questa parte esploreremo le diverse possibilità.

In Francia, la legge obbliga i fornitori di servizi a bloccare l'accesso a quei siti web inseriti in una "lista bloccata" a seguito di una decisione giudiziaria[56] o considerati, dall'Ufficio centrale per la lotta contro la criminalità informatica e le tecnologie della comunicazione, come «aventi contenuti pedopornografici», «collegati ad atti di terrorismo» o passibili di «apologia»[57]. Nell'ottobre 2011, il Tribunal de Grande Instance di Parigi ha ordinato a sette provider francesi di bloccare «per IP o DNS» il sito `copwatchnord-idf.org/`[58], accusato di fare commenti offensivi e diffamatori e di raccogliere dati personali su alcuni agenti di polizia.

In seguito, nel febbraio 2012, il tribunale ha ordinato anche il blocco di uno dei 35 siti mirror[59] che il Ministero dell'Interno voleva colpire[60].

Il tribunale ha deciso invece di non bloccare gli altri 34 mirror,

---

56 République française, 2011, *Loi n. 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure*, article 4.

57 République française, 2015, *Décret n. 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.*

58 Tribunal de grande instance de Paris, 2011, J*ugement en référé du 14 octobre 2011.*

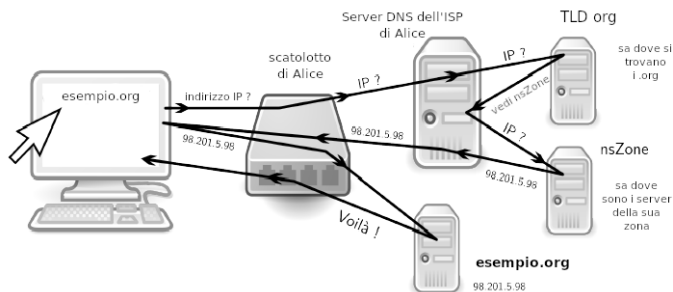
59 Un sito mirror è la copia esatta di un altro sito web.

60 Legalis, 2012, *Ordonnance de référé rendue le 10 février 2012* [nedola.vado.li].

perché il Ministero degli Interni “non ha precisato se aveva tentato o no di identificare gli autori o chi li ospitava”, e di non bloccare neanche gli eventuali mirror che avrebbero potuto comparire in futuro.

### 3.4.1 Bloccare l’accesso al fornitore di risorse

Esaminiamo ora i vari modi per bloccare l’accesso a una risorsa su internet.

**Sequestro di domini**
È possibile deviare il traffico destinato a un certo dominio modificando il registro che associa il nome del dominio all’indirizzo IP, ovvero il DNS[61].

*I passaggi chiave di una richiesta DNS*

Per motivi di efficienza e robustezza, il DNS è gestito da diverse organizzazioni entro un sistema gerarchico e distribuito.

61 Cap. 1.5.1

Il database globale del DNS è ripartito tra vari server, ciascuno dei quali si occupa di gestirne solo una parte. Per esempio tutti i domini che finiscono per .fr fanno capo al DNS dell'AFNIC, un'associazione creata per questo scopo nel 1997. Allo stesso modo, una società americana quotata in borsa (Verisign) ha ricevuto la delega per gestire l'associazione nome/IP di tutti i domini .com.
Un elenco delle organizzazioni e delle aziende responsabili della gestione dei cosiddetti "domini di primo livello" (TLD) come .com, .fr, .org, ecc. si trova sul sito web di IANA[62] (Internet Assigned Numbers Authority) che gestisce il principale server DNS, quello che ha autorità su tutti gli altri.
Se la gestione a livello di TLD è un ruolo puramente tecnico (tenere aggiornato un elenco dei domini di cui sono responsabili), quelli a cui delegano sono solitamente società commerciali (chiamate "registrar"), che vendono i domini.
Noleggiare un dominio è quindi un'operazione diversa da noleggiare un IP. Ad esempio, per creare il proprio sito web: da un lato si dovrà acquistare un dominio, dall'altro trovare l'hosting per il sito, con un relativo indirizzo IP e poi stabilire l'associazione tra i due. Alcune aziende offrono tutti questi servizi contemporaneamente, ma questo non è né sistematico né obbligatorio.
Iniziamo ora a farci una mappa dei punti nevralgici in cui potrebbe intervenire la censura.
Fino ad oggi, il blocco del dominio più spettacolare è stato certamente quello registrato in relazione alla chiusura del sito di file hosting megaupload.com da parte del Dipartimento di Giustizia degli Stati Uniti. Al fine di rendere inaccessibili i servizi, la polizia federale chiese a Verisign (la società che gestisce i .com) di modificare le proprie tabelle di corrispondenze in modo che l'indirizzo non puntasse più verso i server

62 IANA, 2014, *Root Zone Database* [gipino.vado.li].

di Megaupload ma verso quelli della FBI, che rispondevano dicendo che il sito era stato sequestrato[63].
Uno dei primi casi di censura effettuati tramite il blocco del dominio si è verificato nel 2007 a livello di registrar: GoDaddy (il più importante). Nell'ambito di un conflitto tra due suoi clienti, seclists.org e myspace.com, GoDaddy si schierò dalla parte di quest'ultimo e modificò il suo registro DNS rendendo, da un giorno all'altro e senza preavviso, il sito irraggiungibile[64] a chiunque non si ricordasse a memoria l'indirizzo IP.
Infine, se modificare i registri globali è alla portata solo di pochi Stati e aziende, ci sono molti altri che possono semplicemente falsificare i propri server DNS. Ogni Internet Service Provider (ISP) ha generalmente dei propri server DNS che vengono utilizzati di default dai propri abbonati.
Quando un server DNS fornisce informazioni diverse da quelle registrate presso i registrar viene detto "DNS fasullo"[65] e si tratta di una violazione della Net Neutrality[66].
È a questo livello che opera il blocco amministrativo dei siti in Francia: gli ISP devono modificare i loro elenchi per reinstradare gli indirizzi elencati dall'Ufficio centrale per la lotta contro la criminalità legata alle tecnologie dell'informazione e della comunicazione su una pagina del Ministero dell'Interno[67].
Le persone che utilizzano l'ISP Orange hanno potuto sperimentare questo blocco sulla propria pelle il 17 ottobre 2016. A

63 Dopo questa operazione, migliaia di utenti sono stati privati dei propri contenuti in un batter d'occhio (e non parliamo solo di file piratati, ma ci riferiamo alle petizioni online oppure a tutte quelle persone che sostennero che la loro vita professionale fosse rovinata perché non avevano avuto più accesso a documenti personali).

64 Fyodor, 2007, *Seclists.org shut down by Myspace and GoDaddy* [cumepe.vado.li].

65 Stephane Bortzmeyer sviluppa un po' meglio qui il concetto: www.bortzmeyer.org/dns-menteur.html.

66 Cap. 1.4.2

67 *Décret n. 2015-125 du 5 février 2015*, cit.

seguito di un «errore umano», «durante l'aggiornamento dei siti bloccati»[68], il resolver Orange ha dato una risposta "falsa" per un'ora a wikipedia.fr, indicando non i server di Wikipedia, ma una pagina che recitava: «Siete stati reindirizzati a questa pagina del sito del Ministero dell'Interno perché avete cercato di collegarvi a una pagina il cui contenuto incita o condona pubblicamente atti di terrorismo»[69].

## Phishing

Nella stessa ottica, il "phishing"[70] è l'atto di attirare un utente a connettersi a un sito che si finge quello realmente cercato. Ad esempio: esistono siti che somigliano molto a quello di una banca, per indurre l'utente a digitare la sua password al fine di sottrarla e ottenere l'accesso all'interfaccia di gestione dei suoi conti bancari. Per poter fare ciò, l'avversario compra un dominio che a prima vista sembri quello giusto; poi cerca di convincere la persona a connettersi a questo sito, di solito spaventandola, dicendole ad esempio: «Abbiamo rilevato un attacco sul tuo conto» o «Hai superato la tua quota», e poi consiglia di regolarizzare la situazione cliccando sul link incriminato.
Ci sono moltissime tecniche per far sì che il dominio falso assomigli molto a quello vero.
Ad esempio, l'avversario può utilizzare caratteri speciali che assomigliano a quelli dell'alfabeto latino. Così, sostituendo una "e" cirillica con una "e" latina in `example.org`, si ottiene un indirizzo che viene visualizzato in modo (quasi) identico all'originale, ma che rappresenta un indirizzo diverso; a volte si possono trovare dei trattini in più o in meno (ma-banque.fr invece di mabanque.fr); altre volte si utilizza un nome identi-

68 Marc Rees, 2016, *Blocage de Google, OVH et Wikipedia : « on ne cherche pas à vous cacher la vérité » assure Orange*, Nextinpact [bomuza.vado.li].
69 Yannux, 2016, screenshot della paginA del Ministère de l'Intérieur, twitter.com [robute.vado.li].
70 Wikipedia, *Phishing*.

co ma con un dominio TDL diverso (.com, .net, .org, .fr...); alcuni usano anche sottodomini: paypal.phishing.com rimanda a un sito di fishing, non a paypal.com; ecc.
Una contromisura già integrata nei browser consiste nell'avvertire l'utente del pericolo e chiedere conferma prima di accedere ad un sito sospetto. Tuttavia, questa soluzione richiede che il browser contatti ogni volta un database centralizzato che contiene l'elenco dei siti considerati dannosi. E questa soluzione può porre problemi di riservatezza: il server che ospita questo elenco sarà necessariamente a conoscenza delle visite che abbiamo fatto a questo o quel sito.

**Dereferencing**
Infine, un modo semplice ma efficace per impedire l'accesso a un sito web è quello di rimuoverlo dai motori di ricerca e da altre directory: il "dereferencing". In pratica, il sito esiste ancora, ma non compare più sui motori di ricerca (ad es. Google).
In Francia, il dereferencing è una delle tecniche utilizzate per bloccare l'accesso a quei siti web inseriti in una "lista bloccata" a seguito di una decisione giudiziaria o considerati, dall'*Ufficio centrale per la lotta contro la criminalità informatica e le tecnologie della comunicazione*, come «aventi contenuti pedopornografici», «collegati ad atti di terrorismo» o passibili di «apologia di reato»[71]. I motori di ricerca hanno quindi 48 ore di tempo per far sì che questi indirizzi non compaiano più nei loro risultati. Nel 2015 in Francia sono state presentate 855 richieste di cancellazione[72].

---

71 République française, 2015, *Décret n. 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.*
72 Alexandre Linden, 2016, *Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n. 2004-575 du 21 juin 2004 créé par la loi n. 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*, CNIL, p. 9 [casici.vado.li].

### 3.4.2 Attaccare il server

Un altro tipo di attacco consiste per l'avversario nell'impadronirsi del computer che ospita la risorsa che gli interessa. Questo può avvenire fisicamente o a distanza.

**Sequestro del server**
Per un avversario che ne abbia i mezzi, per esempio la polizia o la giustizia, si tratta molto semplicemente di recarsi dove si trova il computer che gli interessa. L'avversario a quel punto può prendersi la macchina oppure copiarsi i dati che ci sono sopra. Successivamente potrà studiare tutte le tracce[73] che sono state lasciate dalle persone che si sono connesse a quella macchina... questo sempre che l'hard-disk non sia cifrato[74].
Tra il 1995 e il 2007 in Europa sono stati sequestrati almeno quattordici server[75]. Nel 2007 un server di Greenpeace Belgio è stato portato via dalla polizia belga in seguito a una denuncia per "associazione a delinquere" fatta da un'azienda elettrica belga contro la quale l'organizzazione ecologista aveva invitato a manifestare.
Più di recente, nella primavera del 2017, un certo numero di server appartenenti alla rete Tor[76] sono stati sequestrati[77], alcuni mantenendoli online e altri no, con il pretesto di un'inchiesta su un attacco informatico che era transitato attraverso quella rete[78].

73 Tomo I, cap. 2
74 Tomo I, cap. 5.1
75 Globenet, 2007, *Les saisies de serveurs en Europe: un historique* [lanopo.vado.li].
76 Cap. 7
77 Guénaël Pépin, 2017, *WannaCrypt: des noeuds Tor saisis par les autorités françaises* [lidito.vado.li].
78 Wikipedia, *WannaCry*.

## Intrusione nei server

Come qualsiasi computer, un server può essere *bucato*: ciò significa che un attaccante può riuscire a introdursi "clandestinamente" all'interno del computer. Errori costitutivi o di programmazione – che permettono di dirottare il funzionamento di un programma e introdursi nel computer dove sta girando – vengono regolarmente scoperti all'interno dei programmi usati correntemente sui server. Sono anche possibili errori di configurazione da parte degli amministratori di sistema. Nell'aprile del 2011, per esempio, degli hacker sono riusciti a introdursi nei server di Sony Online, PlayStation Network e Qriocity (Sony Entertainment Network), sfruttando delle falle all'interno di programmi che ci giravano sopra. Questo ha dato loro accesso ai dati personali e bancari di milioni di utenti della rete di videogiochi[79]: utenti e password, indirizzi fisici e email, ecc.
Se questo esempio ha fatto molto parlare di sé, le falle che rendono possibile questo genere di intrusioni non sono affatto rare e qualsiasi server può venirne coinvolto. Di conseguenza, chi si introduce nel server potenzialmente può accedere a distanza a tutti i dati che ci sono salvati sopra.

## Attacchi DoS

Senza neanche dover sequestrare il server o farvi intrusione, è possibile impedirne il funzionamento saturandolo: l'avversario fa in modo che tantissimi robot cerchino di connettersi tutti insieme, nello stesso momento e ripetutamente, al sito in questione. Dopo un certo numero di richieste, il server[80] viene saturato e non ce la fa più a rispondere: a quel punto il sito risulta inaccessibile. Questo attacco si chiama "Denial of

79 Wikipedia FR, *Piratage du PlayStation Network*; Diowan, 2011, *Retour sur le piratage de Sony* [nudaga.vado.li].
80 Cap. 1.5.3

Service" (DoS)[81]. I robot utilizzati in questo tipo di attacco sono spesso dei software malevoli[82] installati sui computer di persone a loro insaputa.

### 3.4.3 Lungo il tragitto

Infine, un avversario che controlla una parte della rete – come un provider internet – è in grado di ascoltare o manipolare i pacchetti in diversi modi.

**Filtri**
Come abbiamo detto in precedenza[83], un avversario che controlla uno dei router[84] attraverso i quali passa il traffico tra un utente e una risorsa è in grado di leggere più o meno approfonditamente il contenuto dei pacchetti ed eventualmente modificarlo, tanto più se non è cifrato.
Attualmente, quasi tutti i fornitori di accesso a internet attuano questo tipo di analisi, chiamata "Deep Packet Inspection" (DPI)[85], quantomeno a scopo statistico. Inoltre, sempre più di loro, in modo più o meno discreto e più o meno consapevole, lo usano per dare precedenza a determinati pacchetti piuttosto che ad altri, a seconda della destinazione o dell'applicazione a cui corrispondono. Per esempio per rallentare la richiesta di un video, che genera molto traffico (e che quindi a loro costa caro), e privilegiare invece la telefonia VoIP[86]. Questo tipo di metodo è stato per esempio utilizzato dall'ISP SFR[87] per mo-

81 Wikipedia, *Denial of Service.*
82 Tomo I, cap. 3.2
83 Cap. 2.3
84 Cap. 2.3
85 Cap. 3.3
86 Assiste, 2017, *Deep Packet Inspection (DPI)* [cupuce.vado.li].
87 bluetouff, 2013, *SFR modifie le source HTML des pages que vous visitez en 3G* [gegoge.vado.li].

dificare le pagine web visitate dai suoi abbonati tramite 3G[88].
Lo sviluppo massivo di strumenti che permettono questo tipo di analisi approfondita dei pacchetti rende molto più semplice una sorveglianza delle porte di rete degli ISP.
Analizzando questo tipo di dati, i governi possono identificare la posizione di un individuo, quella delle sue relazioni e dei membri di un gruppo per esempio di "oppositori politici"[89].
Sistemi come questi vengono venduti da aziende occidentali alla Tunisia, all'Egitto, alla Libia, al Bahreïn e alla Siria[90], e sono in servizio anche in alcuni Paesi occidentali[91]. Essi permettono, sulla base di una sorveglianza di massa, di individuare degli utenti e di filtrare, o censurare, i contenuti.

**Intercettazioni**

Come nel caso delle care vecchie intercettazioni telefoniche, è assolutamente possibile registrare, del tutto o in parte, dei dati che transitano attraverso una rete: si parla in questo caso di "intercettazioni del traffico IP". Questo permette per esempio di ascoltare tutto il traffico scambiato da un server, o quello che passa da una connessione ADSL domestica.
Se non vengono prese precauzioni particolari, un'intercettazione del traffico IP rivela a un avversario una buona parte delle nostre attività su internet: pagine web visitate, email e loro contenuto, conversazioni in chat… tutto quello che esce dal nostro computer "in chiaro". La cifratura delle comunicazioni rende l'analisi del contenuto intercettato molto più difficile: l'avversario ha comunque accesso ai dati scambiati, ma non può direttamente capirli e utilizzarli. A quel punto può provare a rompere la cifratura… o tentare di aggirare il metodo con cui è stata messa su. Parleremo più avanti delle que-

88 Wikipedia, *3G*.
89 Elaman, 2011, *Communications monitoring solutions* [fucimo.vado.li].
90 Jean Marc Manach, 2011, *internet massivement surveillé* [fodofi.vado.li].
91 Cap. 3.3

stioni legate alla crittografia[92]. In ogni caso, l'avversario avrà comunque accesso a un certo numero di informazioni preziose, come per esempio gli indirizzi IP[93] dei diversi interlocutori coinvolti in una comunicazione.

**Analisi del traffico di rete**

Nel caso in cui il traffico sia cifrato, resta possibile mettere in atto degli attacchi più sottili. Un avversario che può ascoltare il traffico di rete, anche se non ha accesso al contenuto, dispone di altri indizi, come la quantità di informazioni trasmesse in un certo momento.

Per esempio, se Alice invia 2 MB di dati cifrati verso un sito web di pubblicazione, e qualche minuto dopo su quel sito compare un nuovo documento da 2 MB, l'avversario potrebbe facilmente dedurre che, con ottima probabilità, sia stata Alice a pubblicare quel documento. Studiando la quantità di informazioni trasmesse in un unità di tempo, l'avversario può anche tratteggiare una "forma": una sorta di pattern dei dati. Il contenuto di una pagina web cifrata non avrà lo stesso pattern di una conversazione in chat cifrata. Inoltre se lo stesso pattern viene osservato in due punti della rete, l'avversario può supporre che si tratti della stessa comunicazione.

Per fare un esempio preciso: consideriamo un avversario che si trova in ascolto della connessione ADSL di Alice e che osserva del traffico cifrato che non riesce a decifrare, ma che suppone si tratti di Alice che discute su una chat cifrata con Betty. Ipotizziamo che sia in grado di mettere sotto controllo anche la connessione di Betty. Se osserva un pattern simile tra i dati che escono da Alice e quelli che entrano da Betty qualche millisecondo più tardi, avrà avvalorato la sua ipotesi, senza tuttavia disporre di prove formali.

Questo tipo di attacco permette di confermare un'ipotesi pre-

92 Cap. 6

93 Cap. 1.2.5

esistente, ma non di elaborarne una a partire dalle sole informazioni raccolte, a meno che l'avversario non abbia i mezzi per ascoltare *tutta* la rete o che si ponga tra Betty e Alice avendo a disposizione una potenza di calcolo spropositata. L'esistenza di un avversario globale di questo tipo è tecnicamente possibile, ma poco realistico. Tuttavia, agenzie come l'NSA sono capaci di condurre questo tipo di attacchi, almeno all'interno dei loro Paesi: l'NSA dispone di una potenza di calcolo che potrebbe essere sufficiente e alcune voci indicano che ascolterebbe il 75% del traffico internet degli Stati Uniti[94].

### 3.4.4 Attaccare il client

Anche il computer dell'utente può essere bersagliato. Come per un server, un utente malintenzionato può introdursi[95] in un personal computer. Errori di programmazione o altri difetti nel sistema operativo o nelle applicazioni installate a volte consentono agli avversari di eseguire tale hacking – legale o illegale – da internet, senza avere accesso fisico alla macchina. Inoltre, l'intrusione può essere facilitata da cattive pratiche da parte degli utenti, come l'apertura di un allegato email fraudolento o l'installazione di programmi trovati casualmente sul web.
Un rinomato gruppo di hacker tedesco, il Chaos Computer Club, ha messo le mani su uno spyware utilizzato dalla polizia tedesca che ha permesso loro di spiare e controllare un computer a distanza[96]. Tali cookie possono essere installati da remoto e sono autorizzati dalla legge di diversi Paesi.
Ma lo "spionaggio a distanza" non è riservato solo alle prati-

---

94 latribune.fr, 2012, *A peine 25% du trafic web américain échappe à la surveillance du NSA* [nizere.vado.li].
95 Tomo I, cap. 3
96 Mark Rees, 2011, *Le CCC dissèque un cheval de Troie gouvernemental troué*, PCInpact [mosupo.vado.li].

che di polizia. Negli Stati Uniti, per esempio, è stato un liceo a intraprendere un'azione di spionaggio su larga scala: con il pretesto di voler "ritrovare laptop rubati o smarriti", la scuola aveva installato una "funzione" per accendere, per volontà dell'istituto, le webcam di diverse migliaia di computer distribuite agli studenti. Il caso è divenuto di dominio pubblico alla fine del 2009: uno degli studenti era stato accusato di aver tenuto "comportamenti inappropriati", in quell'occasione per uso di sostanze stupefacenti. Il funzionario che aveva accusato lo studente aveva prodotto, come prova, una foto che è risultata essere stata scattata all'insaputa dello studente, dalla webcam del suo computer quando era a casa nella sua stanza[97].

## 3.5 In conclusione

Identificazione dell'utente tramite il suo indirizzo IP, lettura dell'origine e della destinazione dei pacchetti attraverso le loro intestazioni, registrazione di varie informazioni in diverse fasi del percorso, accesso al contenuto vero e proprio degli scambi... tutto questo è più o meno semplice a seconda dell'avversario coinvolto. Un pirata, un pubblicitario, il poliziotto di Saint-Tropez o la NSA non hanno le stesse possibilità, tecniche o legali, di accesso alle tracce menzionate in questo capitolo. Teniamo bene a mente, in conclusione, che il modo in cui Internet è stato progettato – ed è più comunemente usato – è quasi trasparente per a un avversario sufficientemente sveglio... a meno che non si mettano in campo tutta una serie di difese pensate per rendere più difficili queste indiscrezioni. Di queste difese parleremo più avanti in questa Guida.

97 Me, myself and the Internet, 2011, *Mais qui surveillera les surveillants?*

# 4 | Web 2.0

Parlare di Web 2.0 al giorno d'oggi è ormai molto comune. Tuttavia, questa espressione viene perlopiù banalizzata nella discussione generale oppure, al contrario, ne vengono date definizioni troppo tecniche[1] e in questo modo è difficile capire esattamente in cosa consista davvero questo Web 2.0.
Si tratta sostanzialmente di un termine di marketing che definisce l'evoluzione del web in una data epoca, oppure indica la massificazione dell'accesso a internet e la sua conseguente trasformazione in un ghiotto business. Di fatto, nessuna azienda che si occupi di media, comunicazione o commercio può permettersi di ignorarlo: sono obbligate ad adattare il loro modello di business a questo nuovo mercato.
L'arrivo di questi nuovi attori sul web, che finora era composto principalmente da universitari e appassionati, ha trasformato la concezione dei siti web e, di fatto, l'utilizzo che ne fanno gli utenti.
Al di là delle formule di marketing, vogliamo allora provare a vedere più precisamente come queste evoluzioni si manifestano con gli utenti e i cambiamenti topologici[2] che comportano.

## 4.1 Applicazioni internet ricche...

Una delle principali evoluzioni ruota intorno all'interattività dei siti web, che adesso non sono più soltanto delle pagine statiche come quelle di un libro o di una rivista. Grazie all'utilizzo di tecnologie presistenti al Web 2.0 come JavaScript e

---

1 L'esposizione di introduzione alla conferenza di O'Reilly e Battelle sul Web 2.0 citata da Wikipedia è un bell'esempio di definizione troppo tecnica. Wikipedia, *Web 2.0.*

2 Cap. 1.4.3

Flash, i siti web assomigliano sempre di più a delle applicazioni come quelle che troviamo sui nostri computer: sono siti web dinamici[3] che rispondono alle sollecitazioni dell'utente.
Inoltre, la maggior parte dei programmi normalmente installati su un computer sono stati trasposti in versione web e sono accessibili tramite browser. Sono anche apparsi dei sistemi operativi[4], come Chrome OS, concepiti interamente secondo questo principio. Questo spostamento, questo passare dal software installato sul computer al web, è soprattutto una risposta ai problemi di incompatibilità tra software, di licenza e di aggiornamenti.
In effetti non c'è più bisogno di installare nulla: basta una semplice connessione a internet e ci troviamo a disposizione, attraverso il browser, la maggior parte delle applicazioni tradizionali: editor di testi, fogli di calcolo, posta, agenda collaborativa, sistemi per condividere file, player musicali, ecc.
Per esempio Google Drive permette di redigere documenti o fogli di calcolo online. Ma questo servizio consente anche di condividerli con amici, colleghi ecc.
Alcune persone vedono in questa possibilità di accedere a questi strumenti online da "qualsiasi computer, da qualsiasi paese, in qualunque ora"[5] anche un modo di conciliare il lavoro con eventuali problemi medici, metereologici o anche in caso di pandemia ... Non serve più andare in ufficio: "basta un computer connesso a internet per ricostruire immediatamente l'ambiente di lavoro".

---

3 Cap. 1.5.3

4 Tomo I, cap. 1.4.1

5 Lionel Damm et Jean-Luc Synave, 2009, *Entrepreneur 2.0, la boite à outils de la compétitivité... à petit frais* [cucaba.vado.li].

## 4.2 ...e clienti benefattori

Quando sono arrivate sul mercato del web, numerose aziende hanno dovuto rivedere il loro modello economico. L'audience di internet si era ampliata, non era più possibile finanziare un sito web con la sola pubblicità e pagare l'esercito di redattori necessario a fornire contenuti in numero sempre crescente.
I fornitori di servizi hanno utilizzato quindi una tecnica usata sul web già da lungo tempo: contare sulla partecipazione degli utenti. Sono loro, d'ora in poi, a farsi carico di redigere i contenuti che alimenteranno i siti. I fornitori di servizi si accontentano adesso soltanto di ospitare i dati e di offrire l'interfaccia che consente di accedervi. Ma anche – e soprattutto – di aggiungere della pubblicità intorno... e di incassare i soldi.
Per esempio, la piattaforma di condivisione video YouTube in tutti questi anni ha permesso ai propri utenti di caricare e visualizzare video gratuitamente, senza apparentemente chiedere niente in cambio. Adesso, in seguito al successo e forte di questo monopolio, la maggior parte delle persone che vogliono visualizzare e condividere video sono dipendenti da questa piattaforma, cosa che permette a YouTube di imporre a poco a poco l'introduzione della pubblicità: inizialmente la si trovava in un banner a fianco dell'immagine, poi su un banner trasparente sopra l'immagine, finché oggi è proprio un video che viene riprodotto automaticamente prima di quello che volevamo vedere.
Per i fornitori dei servizi, un altro vantaggio di questa soluzione è che gli utenti in questo modo forniscono, più o meno consapevolmente, tutto un insieme di dati[6] che in seguito è possibile monetizzare, soprattutto perché costituiscono dei

---

6 Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat - Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0* [roluzu.vado.li].

profili su cui poi adattare le pubblicità[7].
Succede anche che ormai gli utenti non utilizzino più internet soltanto per scaricare film o leggersi il giornale. Sempre di più, per esempio riempiendo i propri profili Facebook, gli utenti producono contenuti e per così dire li "offrono" alle aziende che forniscono questi servizi. È l'utente stesso a caricare online la playlist di brani musicali che ascolta, le foto delle vacanze in Messico, o anche il corso di storia contemporanea da condividere con i propri compagni di università.
Ovviamente, mentre forniamo i contenuti, stiamo fornendo anche informazioni su di noi, informazioni che gli sguardi indiscreti di pubblicitari e altri avversari[8] non mancheranno di utilizzare.

## 4.3 Centralizzazione dei dati

L'utilizzo di internet come spazio di archiviazione dati va di pari passo con la centralizzazione dei dati degli utenti nelle mani di poche organizzazioni, ubicate in poche località geografiche.
Utilizzare le applicazioni online significa, tra le altre cose, che i documenti non sono più conservati su un personal computer, un hard-disk o una penna USB. Si trovano invece su dei server remoti come quelli di Google[9] o di Ubuntu One, all'interno dei CED, i Centri Elaborazione Dati. Così distanti, da un punto di vista sia geografico che tecnico, che l'utente potrebbe dubitare di averne un qualsiasi controllo. In effetti basterebbe

7 Cap. 3.1.1
8 Cap. 3.1.2
9 Il paragrafo "i vostri contenuti e i nostri Servizi" all'interno delle "Condizioni Generali di Utilizzo" dei servizi forniti da Google dimostra abbastanza chiaramente l'assenza di potere concreto di un utente sui propri contenuti che conserva online. "Ciò che è vostro, rimane vostro", ma Google è libero di farne quel che vuole intanto che glielo lasciamo sui suoi server.

un'assenza di connessione internet e sarebbe già impossibile accedere ai propri documenti, a meno di non averne fatto prima un backup. Questa delocalizzazione dell'archivio rende anche impossibile essere sicuri di cancellare per davvero e in modo sicuro i documenti[10].
La tendenza a migrare i dati e le applicazioni dal nostro computer personale verso internet crea inoltre una "dipendenza dalla connettività". Quando tutta la nostra musica, la rubrica, le mappe stradali della nostra città esistono solo su internet, diventa più difficile immaginare di poter utilizzare un computer offline. Tuttavia, ogni connessione a internet apre delle porte[11]. E più un computer è esposto, più è difficile garantire la sicurezza e l'anonimato dell'utente che vi aveva riposto fiducia.
Non c'è neanche alcuna garanzia che i nostri dati conservati online siano custoditi bene. Anche se un'azienda oggi ci offrisse tutte le sue garanzie di sicurezza (ma, ancora una volta, quale prova abbiamo che le applichi davvero?), potrebbe comunque risultare vulnerabile un domani alla scoperta di una falla[12], oppure un errore di configurazione di un programma potrebbe finire col dare accesso a tutti ai nostri dati. Il rischio è così concreto che è già successo a Dropbox, il servizio di file hosting cifrato online[13].
Le aziende alle quali affidiamo i nostri dati potrebbero anche: chiudere il nostro profilo, decidere di cessare i propri servizi senza che l'utente abbia voce in capitolo, semplicemente fallire, o venire chiusi per problemi legali come nel caso di Megaupload[14].

10 Tomo I, cap. 4.3
11 Cap. 3
12 Cap. 3.4.2
13 Vincent Hermann, 2011, *Dropbox admet posséder un double des clés d'accès aux données* [pilata.vado.li].
14 Cap. 3.4.1

## 4.4 All'interno del server

Nella maggior parte dei casi, le applicazioni online sono sviluppate in modo più chiuso[15] rispetto alle applicazioni libere che possiamo installare sul nostro computer. Quando Google o Facebook decidono di modificare le proprie interfacce, di cambiare i termini del servizio, o di "fare le pulizie", l'utente non ha modo di dire niente.
Inoltre, l'interattività di queste applicazioni web implica che una parte dei loro programmi venga eseguita sul computer client (il nostro), attraverso tecnologie come JavaScript, Flash, o Java[16]. Queste tecnologie vengono ormai attivate di default nei nostri browser, per qualsiasi sito. È smart, pratico e moderno. Ma queste tecnologie, quanto alla sicurezza dei nostri computer e dei nostri dati[17], pongono qualche problemino... È comunque possibile[18] autorizzarne l'utilizzo sito per sito, a seconda di quanto ci vogliamo fidare.

## 4.5 Dalla centralizzazione all'autogestione decentralizzata

Di fronte a una centralizzazione dei dati e delle applicazioni ogni giorno maggiore, come possiamo approfittare dei vantaggi di una rete partecipativa e interattiva senza perdere il controllo sui nostri dati? La sfida è ardua. Ma c'è chi sta lavorando per sviluppare delle applicazioni internet che funzionino in modo decentralizzato presso ciascun utente, invece di essere accentrate su qualche server. Progetti come i social

15 Tomo I, cap. 4
16 Cap. 2.1.3
17 Tomo I, cap. 3.2
18 A seconda del browser che utilizziamo, esistono delle estensioni come noscript (noscript.net) che permettono di gestire questi parametri.

media peer-to-peer, Mastodon[19], Nextcloud[20], la distribuzione YunoHost[21], o ancora internet Cube[22] lavorano in questa direzione.
Attendendo che siano altrettanto semplici da usare quanto le soluzioni proposte dai giganti del Web 2.0, già da adesso è possibile, con un po' di impegno, ospitare da soli la maggior parte dei servizi che vogliamo offrire o utilizzare.

19 https://mastodon.it/
20 https://nextcloud.com/
21 https://yunohost.org/
22 https://internetcu.be/

# 5 | Identità contestuale

Uno dei presupposti di questa guida è il desiderio che le nostre azioni, gesti e pensieri non siano automaticamente – o almeno non del tutto – collegabili alla nostra identità civile.
Pertanto, può essere necessario o semplicemente preferibile sapere a chi ci stiamo rivolgendo: stiamo per intavolare una discussione su un forum o per inviare delle email, per esempio. In questi casi, avere una *identità*, ovvero poter essere identificabili dai nostri corrispondenti, semplifica la comunicazione.

## 5.1 Definizioni

Per iniziare, due definizioni:

- l'*anonimato*, vuol dire non lasciar comparire alcun nome;
- lo *pseudonimato*, vuol dire scegliere e utilizzare un nome differente dal proprio nome civile.

Per come funziona, è molto difficile risultare anonimi o rimanere solo uno pseudonimo su internet.

### 5.1.1 Pseudonimi

Uno pseudonimo, è un'identità diversa da quella assegnata a un individuo dallo stato civile. Possiamo scegliere di farci chiamare Spartaco, Amazzone arrabbiata, Zigouigoui, o anche Mario Rossi. Mantenendo lo stesso pseudonimo durante scambi diversi, i nostri interlocutori avranno buoni motivi per pensare che i diversi messaggi scritti da questo pseudonimo provengano dalla stessa persona: ci potranno rispondere, ma non potranno venirci a malmenare se non sono d'accordo con noi. Bisogna però essere anche consapevoli che anche la scelta stes-

sa di uno pseudonimo potrebbe essere un indizio che permette di risalire alla persona che lo sta utilizzando, almeno nel caso di persone che conoscevano già quello pseudonimo.

### 5.1.2 Identità contestuale

*Riprendendo il filo della nostra storiella introduttiva, l'identità contestuale corrisponderebbe a "una o più persone che vogliono pubblicare delle informazioni sul Sindaco del loro distretto", la persona fisica invece sarebbe in questo caso Benoît.*

Il modo in cui parliamo a seconda delle situazioni, ad esempio se stiamo chiacchierando di arrampicata con persone che condividono con noi questa passione, oppure del nostro lavoro con un impiegato del Centro per l'impiego, oppure con la nostra banca, non sarà sempre lo stesso. In un caso avremo toni più entusiasti e avventurosi, nell'altro piuttosto sobri e seri... parliamo insomma di identità contestuale.
Lo stesso vale quando si utilizza un computer: quando postiamo un messaggio su una chat di incontri, quando annunciamo un grande evento sul proprio profilo Facebook o quando stiamo rispondendo a un'email della mamma, facciamo appello a differenti identità contestuali. Queste identità possono evidentemente mescolarsi e formare un'unica identità composta da tre identità contestuali adatte ai casi di cui sopra: lo scapolo, il festaiolo, il figlio di qualcuno. Queste identità in definitiva fanno tutte parte della personalità del loro proprietario.
Un'identità contestuale insomma è un frammento di una "identità" globale che si suppone corrisponda a una persona fisica, o a un gruppo. È come una fotografia, un'istantanea di una persona o un gruppo, presa da una certa angolazione, a una certa età, ecc.
Essere assolutamente anonimi su internet, è molto complicato:

come abbiamo visto, vengono salvate molte tracce quando si utilizza la rete[1]. Questo fenomeno è tanto più vero con i social media, per i quali delineare un'identità unica e tracciabile ha uno scopo economico[2]. È impossibile non lasciare nessuna traccia, ma è possibile lasciare tracce che non portano a niente. Incontreremo delle difficoltà simili anche quando facciamo la scelta dello pseudonimato: più utilizziamo uno pseudonimo, più le tracce che lasciamo si accumulano. Piccoli indizi che una volta raggruppati permettono di rivelare l'identità civile che corrisponde allo pseudonimo.

## 5.2 Dall'identità contestuale all'identità civile

Esistono diversi modi, più o meno offensivi, per rendere inefficace uno pseudonimo o per svelare i collegamenti tra un'identità contestuale e la/le persone fisiche che l'utilizzano. Esistono diversi modi, più o meno offensivi, per rendere inefficace uno pseudonimo o per svelare i collegamenti tra un'identità contestuale e la/le persone fisiche che l'utilizzano.

### 5.2.1 Il controllo incrociato

Partiamo dall'esempio precedente delle tre identità contestuali[3]: è legittimo domandarsi cosa comporti, in termine di anonimato, questo destreggiarsi tra le differenti identità. Se vogliamo utilizzare uno pseudonimo invece del nostro nome civile, potrebbe essere più adatto avere un'identità (dunque uno pseudonimo) per ciascun contesto: uno per le chat di incontri, un altro per i social media, uno per le relazioni fa-

---

1 Cap. 2
2 Ippolita, 2012. *Nell'acquario di Facebook.*
3 Cap. 5.1

miliari, ecc. in modo da evitare il controllo incrociato. Se le informazioni che escono da queste identità non sono compartimentate, cioè se stiamo usando lo stesso pseudonimo, un controllo incrociato permetterà di restringere il campo sulle persone a cui potrebbero corrispondere. In questo modo diventa più facile tracciare un legame tra una presenza digitale e una persona fisica, e quindi dare un nome civile all'identità contestuale corrispondente.

Prendiamo per esempio un utente che utilizza lo pseudonimo bruce76 su un blog in cui racconta di essere vegetariano e amare i film d'azione. Esistono solo un certo numero di persone che corrispondono a questi criteri. Aggiungiamoci che lo stesso pseudonimo viene utilizzato per organizzare attraverso un social network una festa in una tale città e per comunicare via email con la Signora Qualcuno. Indubbiamente non ci sono tante persone vegetariane, che amano i film d'azione, che hanno organizzato una festa in quella città e che comunicano via email con la Signora Qualcuno.

Più uno stesso pseudonimo viene usato per tanti e vari contesti, più si restringe il numero delle persone che possono corrispondere a quello pseudonimo. In questo modo, facendo dei controlli incrociati, si riesce a depotenziare o annullare lo pseudonimato.

Questo è quello che molti utenti di AOL hanno scoperto a loro spese quando sono stati pubblicati più di tre mesi di risultati dell'utilizzo del motore di ricerca dell'azienda[4]. Molti ricercatori hanno facilmente fatto cadere il fragile pseudonimato applicato da AOL su questi dati. Lo stesso governatore del Massachusetts ha fatto le spese di questo controllo incrociato, quando la sua cartella medica, in teoria anonimizzata, è stata identificata in mezzo a quella di tutti gli altri cittadini. La ricercatrice che ha presentato questa dimostrazione sulla dea-

4 Nate Anderson, 2006, *AOL releases search data on 500,000 users* [gatici.vado.li].

nonimizzazione dei dati, ha avuto anche l'ironia di spedirgli la sua cartella clinica via posta[5].

### 5.2.2 Correlazione temporale

Un po' più tecnica, la correlazione temporale permette anch'essa di far cadere o rendere fragile l'anonimato o lo pseudonimato. Se in un intervallo di tempo ristretto avviene per esempio una connessione sia alla casella di posta a`mazzone@esempio.org` sia a quella di `maria.rossi@libero.it`, la probabilità che queste due caselle facciano riferimento alla stessa persona aumenta, tanto più se questo fatto si ripete. Più avanti espliciteremo varie risposte che è possibile dare a questo problema, a seconda dei diversi bisogni.

### 5.2.3 Stilometria

È possibile applicare analisi statistiche sullo stile di qualunque tipo di dato, soprattutto sui testi. Analizzando[6] le differenti caratteristiche di un testo, come la frequenza di parole funzione[7], la lunghezza delle parole, delle frasi e dei paragrafi, la frequenza della punteggiatura, si possono fare delle comparazioni tra testi anonimi e non, traendone degli indizi sugli autori.
Questo tipo di analisi per esempio è stata utilizzata all'interno

---

5 Paul Ohn, 2009, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* [zelufi.vado.li].

6 Ad esemio grazie a dei software come *The Signature Stylometric System* [cosadi.vado.li] o *Java Graphical Authorship Attribution Program* [gugano.vado.li].

7 Le parole funzione sono parole il cui ruolo sintattico è più importante del significato. Queste sono in genere parole di collegamento. Cfr. *Wikipedia, Parole funzione*.

del processo a Theodore Kaczynski[8], per accreditare il fatto che fosse l'autore del manifesto "La società industriale e il suo futuro"[9].
Gli autori di uno studio recente[10] hanno cercato di "simulare un tentativo di identificazione dell'autore di un blog anonimo. Se l'autore è abbastanza prudente da evitare di rivelare il proprio indirizzo IP o altri identificativi espliciti, il suo avversario (per esempio un censore governativo) può ricorrere all'analisi del suo stile di scrittura". Le loro conclusioni mostrano che la stilometria permette di ridurre fortemente, attraverso moltissime possibilità, il numero degli autori possibili di un testo anonimo – la precisione aumenta ovviamente all'aumentare del numero di campioni "firmati" (cioè quelli in cui l'autore è noto) forniti al software di analisi.
Più spesso, questo permette di restringere il campo degli autori possibili passando da 200 a 100, su 100.000 iniziali. "... aggiunta a un'altra fonte d'informazione, questa potrebbe essere sufficiente a fare la differenza tra l'anonimato e l'identificazione di un autore". Al momento in cui scriviamo queste righe, nel 20% dei casi è anche possibile identificare direttamente l'autore anonimo.
La particolarità di questo lavoro è che va oltre il quadro dei piccoli campioni (un centinaio di possibilità) a cui si erano confinati gli studi precedenti, e si interessa invece all'identificazione dell'autore in mezzo a un numero molto ampio di possibilità. In altre parole, dimostra che la stilometria può essere impiegata per confermare l'origine di un testo all'interno di un range di possibilità molto alto.

---

8 Kathy Bailey, 2008, *Forensic Linguistics in Criminal Cases, Language in Social Contexts* [tatenu.vado.li].

9 Theodore Kaczynski, 1998, *La société industrielle et son avenir* [ribuze.vado.li].

10 Hristo Paskov, Neil Gong, John Bethencourt, Emil Stefanov, Richard Shin, Dawn Song, 2012, *On the Feasibility of internet-Scale Author Identification* [vabezi.vado.li].

Nonostante ciò, scrivere cercando di mascherare il proprio stile, anche senza avere particolari conoscenze, sembra sia in grado di rendere inefficaci le analisi stilografiche. Imitare lo stile di qualcun altro permette di renderle vane in più della metà dei casi[11].
Altri ricercatori hanno inoltre sviluppato dei programmi che suggeriscono le modifiche da effettuare per rendere anonimo un testo[12].

## 5.3 La compartimentazione

Come abbiamo visto, esistono numerose possibilità di attacco che permettono di riuscire a far corrispondere un'identità civile a una contestuale. L'utilizzo sempre dello stesso nome per le nostre varie attività, senza dubbio è la pratica che più facilmente rischia di tradirci.
È quindi importante riflettere bene sull'uso che facciamo dei nostri pseudonimi. È molto pericoloso riunire varie identità contestuali sotto lo stesso pseudonimo. La migliore prevenzione resta quella di separarle chiaramente fin da subito in modo da evitare noie in futuro. Dopo tutto, una pratica o un'identità che può venire utilizzata in un dato momento può all'improvviso trasformarsi in una fonte di problemi per motivi che non potevamo prevedere.
Nonostante ciò, queste pratiche non sono sempre facili da mettere in campo. Anche perché ancor più delle tecniche

11 M. Brennan, R. Greenstadt, 2009, *Practical attacks against authorship recognition techniques, dans Proceedings of the Twenty-First Innovative Applications of Artificial Intelligence Conferenc*e [furica.vado.li].
12 Andrew W.E. McDonald, Sadia Afroz, Aylin Caliskan, Ariel Stolerman, Rachel Greenstadt, 2012, *Use Fewer Instances of the Letter "i": Toward Writing Style Anonymization*, The 12th Privacy Enhancing Technologies Symposium [rezave.vado.li].

descritte precedentemente[13], la separazione tra queste differenti identità contestuali dipende da molti altri parametri. Soprattutto dalle relazioni che stabiliamo con le altre persone, relazioni digitali o no. Non è detto che sia facile avere un'identità contestuale differente per ogni singola sfaccettatura della nostra personalità o per ciascuna delle nostre attività. Né è facile evitare che si mescolino tra loro. Queste identità si evolvono in base alle attività che svolgiamo tramite esse e con lo scorrere del tempo. Per più tempo le utilizziamo, più risulterà difficile tenere separati gli ambiti. È quindi tutt'altro che semplice mantenere un equilibrio e misurare gli sforzi necessari a mettere in campo queste identità multiple con i loro sperati benefici. Tanto più che in questo contesto è difficile poi fare marcia indietro.
Alcuni strumenti come i social media le rendono del resto quasi impraticabili, obbligandoci a una trasparenza assoluta.

## 5.4 I social media: centralizzazione delle funzioni e identità unica

In effetti i social media tendono a centralizzare delle funzioni che in passato erano assicurate da differenti strumenti: dallo scambio di messaggi alla pubblicazione di storie, passando dai gruppi di discussione. Tendono a sostituirsi sia alle email che alla messaggistica istantanea, ai blog e ai forum.
Contemporaneamente vengono sviluppate nuove funzioni, come una certa vita relazionale digitale o l'esistenza di una comunicazione più importante del contenuto stesso, spinta all'estremo con i "poke", messaggi senza contenuto[14]. Il Web

13 Cap. 5.2
14 Fanny Georges, 2008, *Les composantes de l'identité dans le Web 2.0, une étude sémiotique et statistique*, Communication au 76ème congrès de l'ACFAS [sefame.vado.li].

2.0 incoraggia ad esprimersi su argomenti che in passato sarebbero stati considerati intimi[15].
E infine, niente di nuovo sotto il sole, riecco la centralizzazione di molte funzioni e pratiche verso un unico strumento. È proprio questo “tutto in uno” di tali piattaforme, la loro grafica e la facilità di utilizzo a renderle così di successo. Ma questa centralizzazione pone delle questioni riguardo alle conseguenze dell’utilizzo di questi strumenti sulla nostra intimità.
La pressione sociale che ci spinge a utilizzare i social media è molto forte in certi ambienti: quando dei gruppi li utilizzano nella maggior parte delle loro comunicazioni, dai messaggi personali agli inviti pubblici fino alla pubblicazione di informazioni, non partecipare ai social media significa venire emarginati. Il successo di questi siti poggia sull’effetto rete: più gente li utilizza, più è importante starci.
Allo stesso tempo, questi social media permettono anche di fuggire da queste pressioni di gruppo e assumere o sperimentare più facilmente certe parti della propria personalità che non necessariamente questi gruppi ritengono accettabili.
La centralizzazione di tutte le attività su una sola piattaforma rende estremamente difficile l’utilizzo di pseudonimi differenti per differenti identità contestuali. In effetti, facendo convergere tutte le informazioni nello stesso luogo, il rischio di mescolare tutte le identità viene massimizzato. Gran parte dei social media richiedono un’identità unica: quella corrispondente all’identità civile di una persona fisica. Questa è una differenza chiave rispetto a un modello in cui un individuo può avere diversi blog con toni e contenuti differenti, ciascuno con un diverso pseudonimo. Oltretutto, come per i siti d’incontri, dove più si è onesti e migliori sono i risultati, in questo contesto più contenuti forniamo, più utilizziamo la piattaforma e

15 Alain Rallet, Fabrice Rochelandet, 2010, *La régulation des données personnelles face au web relationnel: une voie sans issue?*, Réseaux numéro 167, Données personnelles et vie privée [bodose.vado.li].

migliori sono le interazioni.
Tanto più che l'utilizzare il proprio nome civile fa parte delle regole di uno strumento come Facebook, che impiega diversi meccanismi per smascherare gli pseudonimi[16]. Queste aziende spingono al limite il modello di business della pubblicità mirata e della vendita delle profilazioni: "mettono in atto differenti processi tecnici per individuare l'identità degli utenti, a partire dall'identità basata sulle loro dichiarazioni, fino all'identità che agisce[17] e l'identità calcolata, fondata sull'analisi comportamentale: siti visitati, numero di messaggi, ecc. Sembra insomma che l'anonimato completo diventi impossibile in un universo virtuale in cui gli utenti sono prima di tutto dei consumatori da osservare"[18].
Nel luglio 2011, Max Schrems invocando una direttiva europea è riuscito a ottenere l'insieme dei dati di cui Facebook disponeva su di lui. Il dossier che ha ricevuto comprendeva 1222 pagine[19], che includevano non soltanto l'insieme delle informazioni disponibili sul suo profilo, ma anche tutti gli eventi ai quali era stato invitato (compresi gli inviti declinati), tutti i messaggi ricevuti e inviati (compresi quelli cancellati), tutte le foto caricate su Facebook accompagnate da metadati[20] che riguardavano soprattutto la geolocalizzazione, tutti i poke mandati o ricevuti, tutti gli "amici" (compresi gli "amici" cancellati), i log di connessione a Facebook (incluso l'indirizzo IP e la sua geolocalizzazione), tutti i dispositivi (identificati tramite un cookie[21]) utilizzati dal profilo, e anche gli altri profili che hanno utilizzato gli stessi dispositivi, e pure la localiz-

16 Revoltenum, 2012, *Facebook incite à la délation* [raroli.vado.li].
17 Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat - Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0* [soriga.vado.li]
18 Robert Panico, 2010, *Approches sociologiques* [pazipa.vado.li].
19 Europe versus Facebook, 2012, *Facebook's Data Pool* [lipagi.vado.li].
20 Tomo I, cap. 2.6
21 Cap. 2.1.2

zazione della sua ultima connessione a Facebook (longitudine, latitudine, altitudine).
Infine, malgrado le dichiarazioni del fondatore di Facebook, come quella che "l'era della vita privata è finita"[22], ci sono ancora molte strategie da sviluppare e riprogettare per giocare con i vari margini rimasti ancora attuali. Questo sempre nell'ottica di riuscire ad avere un po' di presa sulle domande fondamentali: "Cosa vogliamo mostrare?", "Cosa accettiamo di rendere visibile?" e "Cosa vogliamo nascondere e a quale prezzo?".

22 Bobbie Johnson, 2010, *Privacy no longer a social norm, says Facebook founder* [piruzi.vado.li].

# 6 | Celare il contenuto delle comunicazioni: la crittografia asimmetrica

Nel primo tomo di questa guida, abbiamo visto che la strategia più seria per proteggere dei dati dagli sguardi indiscreti è la crittografia[1]: essa permette di renderli leggibili soltanto a chi possiede la chiave segreta.

## 6.1 Limiti della crittografia simmetrica

Nel quadro della crittografia simmetrica , è la stessa chiave segreta che permette di effettuare sia la cifratura che la decifratura.
La crittografia simmetrica[2] è perfetta nel caso si voglia cifrare una penna USB o un altro supporto di archiviazione.
Tuttavia, nel caso di una comunicazione, dato che la persona che deve decifrare i dati non è la stessa di quella che li ha cifrati, si pongono numerosi problemi:
Innanzitutto, occorre una nuova chiave segreta per ciascuna coppia mittente/ricevente: se voglio poter scambiare dei messaggi cifrati allo stesso tempo sia con mia sorella che con un amico, avrò bisogno di usare due chiavi differenti, altrimenti mia sorella potrebbe decifrare i messaggi che scambio con il mio amico e viceversa.
Inoltre mittente e destinatario devono mettersi d'accordo su una chiave segreta e scambiarsela in modo riservato. Se un avversario entrasse in possesso di questa chiave segreta, potrebbe decifrare non solo tutti i nostri scambi passati, ma anche quelli futuri. In tal caso sarebbe necessario, per quanto difficile, che il nostro interlocutore fosse avvertito in modo

1 Tomo I, cap. 5
2 Tomo I, cap. 5.4.1

sicuro (quindi autenticandoci) che il segreto è stato svelato. Supponiamo di ricevere un messaggio che dice "la chiave non è più sicura": se fosse vero, bisognerebbe smettere di utilizzare questo mezzo di comunicazione. Oppure: un avversario che volesse disturbare le nostre comunicazioni potrebbe allo stesso modo mandare questo messaggio e centrare l'obiettivo senza grandi sforzi (ecco perché sarebbe importante autenticarsi). La crittografia asimmetrica risolve queste problematiche... ma ne presenta altre.

## 6.2 Una soluzione: la crittografia asimmetrica

Negli anni 70, dei matematici hanno rivoluzionato la crittografia trovando una soluzione ai problemi posti dalla crittografia simmetrica[3] creando la crittografia *a*simmetrica. È detta "asimmetrica" perché per decifrare un messaggio utilizza una chiave diversa da quella con cui è stato cifrato.
Prendiamo l'esempio di Alice: lei vorrebbe ricevere un messaggio cifrato da parte di Betty. Alice invia a Betty un lucchetto aperto, di cui custodisce gelosamente la chiave, e invia la sua chiave pubblica a Betty.

*Alice invia la sua chiave pubblica a Betty*

3 Tomo I, cap. 5.1

Betty allora infila il suo messaggio in una scatola e utilizza il lucchetto per chiuderla – non ha bisogno della chiave del lucchetto per farlo:

*Betty cifra un messaggio*

Betty poi invia ad Alice la scatola contenente il messaggio, protetta dal lucchetto chiuso:

*Betty invia un messaggio cifrato*

Grazie alla chiave, che per tutto questo tempo ha custodito a casa sua, Alice può aprire il lucchetto:

*Alice decifra il messaggio cifrato*

Come si vede, grazie alla crittografia asimmetrica, le sole cose che transitano attraverso la rete sono un lucchetto aperto prima e un lucchetto chiuso dopo. E se una persona malintenzionata dovesse incappare nel lucchetto aperto, non sarebbe così grave: non avrebbe comunque ottenuto la possibilità di aprire il lucchetto chiuso.

### 6.2.1 Chiave pubblica, chiave privata

Questo tipo di cifratura è anche chiamato "cifratura a chiave pubblica". Il lucchetto aperto di Alice è la sua "chiave pubblica", viene chiamata così perché non è necessario nasconderla: può essere resa pubblica, per esempio pubblicata su internet, in modo che ogni persona che voglia scrivere ad Alice in modo cifrato possa procurarsela.
Al contrario, la chiave del lucchetto, lo strumento che serve ad Alice ad aprire il lucchetto chiuso che protegge il messaggio, non deve mai finire nelle mani dell'avversario. Alice la custodisce gelosamente, al riparo dagli sguardi indiscreti: si tratta di quello che viene definito "chiave privata".
Chiave pubblica e chiave privata formano la coppia di chiavi di Alice. Chiunque voglia farsi inviare messaggi cifrati in maniera asimmetrica deve disporre di una propria *coppia di chiavi*.

### 6.2.2 Una questione di numeri primi...

Nel mondo reale, la chiave pubblica e la chiave privata non sono altro che dei numeri. Una chiave permette di decifrare ciò che è stato cifrato con l'altra chiave:

Ma com'è possibile che la chiave pubblica permetta di cifrare un messaggio senza che permetta anche di decifrarlo? La crittografia asimmetrica si basa su alcuni problemi matematici estremamente difficili da risolvere. L'algoritmo di cifratura RSA, per esempio, si basa sulla "fattorizzazione dei numeri interi". Ovvero la scomposizione di un numero intero in numeri primi.

Se prendiamo per esempio il numero 12, troveremo che è semplice scomporlo in $2 \times 2 \times 3$. Oppure, 111 è scomponibile in $3 \times 37$. Ma come si scompone il seguente numero di 232 cifre? 1230186684530117755130494958384962720772853569595334 7921973224521517264005072636575187452021997864693899564749427740638459251925573630345373154826850791702612214291346167042921431160222124047927473779408066535141959745 9856902143413. Il risultato è il prodotto di due numeri primi formati ciascuno da 116 cifre.

Il problema della fattorizzazione degli interi viene studiato dai matematici da più di duemila anni e tuttavia non è stata tro-

vata ancora una soluzione pratica: il miglior metodo continua ad essere quella di provare con tutti i numeri primi possibili. Con un computer attuale, questo calcolo durerebbe ben più di una vita umana[4]. I numeri più difficili da fattorizzare sono i prodotti di due grandi numeri primi. Vengono quindi scelti dei numeri grandi a tal punto che anche dei computer estremamente potenti non siano in grado di calcolare la fattorizzazione in un tempo realistico.
Il fare affidamento su questo metodo si basa quindi sulla speranza che il nostro avversario disponga di una potenza di calcolo relativamente limitata. La grandezza delle chiavi, che si misura in bit, è insomma di capitale importanza. In effetti, se consideriamo che una chiave asimmetrica da 2048 bit[5] è sicura fino al 2030[6], una chiave da 512 bit viene rotta in qualche mese con un computer attuale di fascia alta[7]. Bisogna tenere presente che ciò che è "bucabile" in dieci anni con un computer potrebbe esserlo in un anno con dieci computer identici al primo. In più, se un giorno qualcuno risolvesse il problema matematico della fattorizzazione degli interi, sarebbe possibile decifrare senza troppa difficoltà gli scambi cifrati archiviati fino a quel momento – questo tipo di raccolta dati fa parte delle varie attività dell'NSA, agenzia d'intelligence statunitense[8]. Molti dei

---

4 La fattorizzazione di questo numero di 768 bit nel 2010 ha comportato 20^10 operazioni. I ricercatori che l'hanno realizzato stimano che il calcolo richiederebbe circa 2000 anni con un processore AMD Opteron a 2.2 GHz, il che corrisponde a diverse centinaia di anni su un processore all'ultimo grido (Thorsten et al., 2010, *Factorization of a 768-bit RSA modulus* [moleru.vado.li]).

5 Un bit è una cifra binaria (0 o 1). Per saperne di più: Wikipedia, *Bit*.

6 Agence nationale de la sécurité des systèmes d'information, *Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [zicasi.vado.li].

7 S. A. Danilov, I. A. Popovyan, 2010, *Factorization of RSA-180* [zacuvi.vado.li].

8 Nicole Perlroth, Jeff Larson, Scott Shane, 2013, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, The New York Times [pivetu.vado.li].

segreti militari e commerciali diventerebbero quindi accessibili per chi avesse accesso agli archivi. In altri termini, una terribile sventura per aziende concorrenti e intelligence nemiche...
Intanto, gli attacchi utilizzati finora contro i sistemi di crittografia asimmetrica sono rivolti a sfruttare un errore nel codice[9] di questo o di quel programma, e non prendono di mira il principio matematico del sistema.

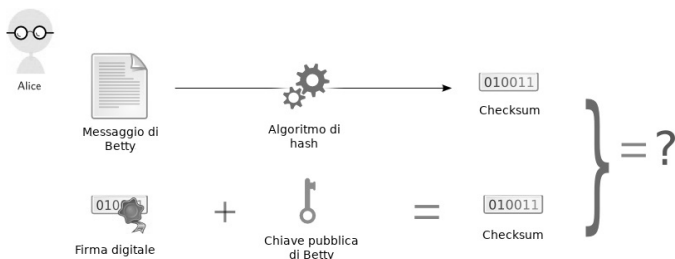
## 6.3 La firma digitale

La coppia di chiavi utilizzata per la crittografia asimmetrica può anche essere utilizzata per provare l'autenticità di un messaggio. Come funziona? Riprendiamo l'esempio di Betty che invia un messaggio ad Alice. Questa volta Betty vuole mettere una firma digitale al proprio messaggio in modo che Alice possa essere sicura dell'identità dell'autrice.
Nel primo volume di questa guida, abbiamo parlato del checksum[10]: un numero che consente di verificare l'integrità di un messaggio. Questa impronta serve anche a firmare dei dati digitali. Per prima cosa il computer di Betty calcola un checksum del messaggio che sta per mandare ad Alice.
In seguito, questa impronta viene cifrata con la chiave privata di Betty: questa è la firma digitale. E sì: l'impronta viene cifrata con la chiave privata di Betty, a cui nessun altro ha accesso, e non con la chiave pubblica di Alice. Questa firma serve ad autenticare il mittente, non il destinatario. Ora, abbiamo detto che la chiave pubblica e la chiave privata sono due numeri scelti in modo che l'uno permetta di decifrare ciò che l'altro ha cifrato. Niente ci impedisce quindi di cifrare qualcosa con la chiave privata. In questo caso sarà la chiave pubblica a decifrarlo.

9 Tomo I, cap. 4
10 Tomo I, cap. 5.2

Betty invia allora il messaggio accompagnato dalla propria firma ad Alice.

*Betty fimra un messaggio*

Per verificare la firma il computer di Alice controlla il checksum del messaggio e in parallelo decifra la firma.

*Alice verifica il messaggio*

Dato che è stata cifrata con la chiave privata di Betty, per decifrare questa firma è sufficiente la chiave pubblica di Betty. Se il checksum del messaggio ricevuto corrisponde alla firma decifrata (che, come abbiamo detto, non è nient'altro che il checksum del messaggio calcolato dal computer di Betty), Alice è sicura dell'autenticità del messaggio che ha ricevuto. Betty conserva la propria chiave privata in un luogo sicuro. È quindi l'unica in grado di cifrare il checksum che Alice ha decifrato con la chiave pubblica di Betty.
Il lato negativo di questa certezza è che chi possiede una chiave privata difficilmente potrà negare di essere l'autore del messaggio.

## 6.4 Verificare l'autenticità della chiave pubblica

La crittografia asimmetrica permette di cifrare e firmare messaggi senza aver bisogno di essersi scambiati prima un segreto condiviso.
Nonostante ciò, non risolve una questione importante: come ci si assicura che quella che possediamo è la *vera* chiave pubblica del destinatario e non è invece quella di un usurpatore che vuole intercettare i nostri messaggi?

### 6.4.1 L'attacco Man in the Middle

Riprendiamo l'esempio di Alice che vuole ricevere un messaggio cifrato da parte di Betty, nonostante la presenza di un'avversaria, Carola, che è in grado di avere accesso ai messaggi scambiati:

- Alice inizia inviando la propria chiave pubblica a Betty. Carola la può leggere.

- Betty cifra il proprio messaggio con la chiave pubblica che ha ricevuto, poi lo spedisce ad Alice.
- Carola, che non possiede la chiave privata di Alice, ma soltanto la chiave pubblica, non può decifrare il messaggio.
- Alice invece, può decifrare il messaggio con la sua chiave privata che custodisce con cura.

Ma se Carola è in grado di modificare gli scambi tra Alice e Betty, le cose si complicano:

- Quando Alice invia la propria chiave pubblica a Betty, Carola l'intercetta e al posto di quella di Alice rimanda a Betty una propria chiave pubblica di cui ha la corrispondente chiave privata.
- Betty cifra il suo messaggio con la chiave pubblica che ha ricevuto e poi lo manda ad Alice. Ma la chiave che ha ricevuto appartiene a Carola: l'ha sostituita a quella di Alice.
- Carola intercetta di nuovo il messaggio. Questa volta però è cifrato con la sua chiave pubblica, di cui ha la chiave privata. A questo punto è in grado di decifrare il messaggio per leggerlo e eventualmente modificarlo. In seguito cifra di nuovo il messaggio con la vera chiave pubblica di Alice e poi lo manda ad Alice.
- Alice quindi riesce a decifrare il messaggio con la propria chiave privata senza accorgersi di niente.

In questo modo Betty è convinta di utilizzare la chiave di Alice, mentre invece sta utilizzando quella di Carola. Allo stesso modo, Carola può sostituire la chiave pubblica di Betty e falsificare la firma del messaggio trasmesso da Betty ad Alice. Alice riceverà un messaggio cifrato e debitamente firmato.... da Carola.
Questo attacco informatico si chiama Man in the Middle (o

MitM)[11]. Nel nostro esempio, Carola era "l'uomo nel mezzo", capace di leggere e modificare la comunicazione cifrata facendosi passare, agli occhi di ciascun lato della comunicazione, per l'altro.
Un avversario può mettersi nella posizione del Man in the Middle in vari modi.
I fornitori di accesso a internet (ISP) per esempio sono particolarmente ben posizionati, perché tutto il traffico passerà obbligatoriamente tramite loro. Anche un *grosso* nodo della rete, per il quale passa una quantità importante di traffico, sarà in grado di mettere in atto questo attacco[12]. Infine un avversario che ha accesso alla rete locale che state utilizzando, potrà far transitare il traffico dal suo computer utilizzando delle tecniche più specifiche[13].
Per premunirsi contro questo attacco, occorre che Betty abbia modo di verificare che la chiave pubblica che sta utilizzando sia davvero quella di Alice. La chiave pubblica non è un'informazione confidenziale, bisogna quindi controllare la sua *autenticità* prima di utilizzarla.
Quando è possibile, il modo più semplice per Betty è quello di incontrare Alice in modo da verificare che la chiave pubblica di cui dispone sia davvero la sua. Anche se Carola è presente al momento dell'incontro non importa: avverrà solo la verifica della chiave pubblica, non verrà scambiato nessun segreto (tranne il fatto che Betty e Alice hanno intenzione di comunicare, ma questo, vista la sua posizione, Carola l'avrebbe saputo lo stesso). Una volta fatta questa verifica, si potrà effettuare una cifratura end-to-end tra Alice e Betty. Una cifratura viene definita end-to-end quando avviene tra sorgente e destinatario senza interruzioni. La cifratura avviene nel

---

11 Wikipedia, *Attacco Man in the Middle.*

12 reflets.info, 2011, *#OpSyria: Bluecoat au coeur d'attaque MITM de grande envergure?* [mapame.vado.li].

13 Wikipedia, *ART poisoning.*

computer di Alice e la decifratura in quello di Betty. Tra le due circolerà un messaggio dal contenuto cifrato, e a transitare in chiaro sarà soltanto l'intestazione della comunicazione[14], una richiesta HTTP o un'email.
Tuttavia capita spesso che Betty non possa incontrare Alice – a maggior ragione nel caso in cui non si conoscano: incontrando una persona che si presenta come Alice, Betty non potrebbe essere sicura che si tratti davvero di lei. Questo è il caso in cui ci imbattiamo quando vogliamo cifrare le nostre comunicazioni verso un sito web: generalmente non conosciamo affatto le persone che ci stanno dietro.

### 6.4.2 Infrastrutture a chiave pubblica

La principale soluzione correntemente utilizzata è quella di disporre di autorità fidate che certificano le chiavi pubbliche firmandole[15]: si parla in questo caso di *certificati*. Alice chiede a un'autorità di certificare la sua chiave pubblica[16], spesso pagando. L'autorità verifica l'identità di Alice, per esempio chiedendogli la sua carta d'identità, poi firma la sua chiave.
Prima di utilizzare la chiave di Alice, Betty (o meglio il suo computer) verifica che sia firmata da un'autorità che considera degna di fiducia. Si parla in questo caso di "infrastruttura a chiave pubblica" (Public Key Infrastructure, o PKI).
Questo è il principio correntemente utilizzato per autenticare i siti web o i provider di posta elettronica con i quali il computer stabilisce una connessione cifrata[17]. I problemi più comuni quando si stabilisce una connessione cifrata verso un sito web sono la protezione delle password – per connettersi alla pro-

---

14 Cap. 2.4.1
15 Cap. 6.3
16 Cap. 6.2.1
17 Cap. 1.4.2

pria casella di posta, per esempio – o la protezione dei dati bancari – per effettuare acquisti su siti di vendita online. Il protocollo[18] utilizzato per questo tipo di cifratura è chiamato TLS (in precedenza SSL)[19].
Tuttavia, questo tipo di soluzione non fa che spostare il problema: bisogna aver fiducia nell'autorità di certificazione, la Certification Authority (CA). In generale si tratta di aziende commerciali, più raramente enti pubblici.
Per questa ragione Microsoft, Apple e Mozilla includono ciascuna delle Certification Authority governative all'interno di quelle riconosciute dai loro browser[20]. Mozilla Firefox include[21] in particolare Certification Authority governative (cinese, catalana, spagnola, olandese, turca), aziende di certificazione (Entrust, GoDaddy, Verisign) e aziende di telecomunicazione (Amazon, Deutsche Telecom, Google).
Firefox include anche l'Authority dell'internet Security Research Group. Questo gruppo ha sviluppato Let's Encrypt[22], una Certification Authority gratuita, libera e automatizzata. Lanciata nel 2016, semplifica l'accesso a dei certificati validi per i piccoli server.
Ma i governi, che spesso hanno la possibilità di mettersi nella posizione del Man in the Middle[23], hanno il potere anche di indicare qualunque certificato come valido, firmandolo con la

---

18 Cap. 1.2

19 Quando vogliamo cifrare una connessione con un server web o di posta, utilizziamo il protocollo TLS. Si tratta di uno standard che permette di incapsulare il protocollo utilizzato abitualmente. Per esempio il protocollo web HTTP, quando viene incapsulato in quelo TLS e dunque cifrato, viene chiamato HTTPS. Lo stesso avviene con i protocolli di posta POPS, IMAPS e SMTPS.

20 Christopher Soghoian, Sid Stamm, 2011, *Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [sesifu.vado.li].

21 Common CA Database, 2017, *CA Certificates In Firefox* [puzita.vado.li].

22 https://letsencrypt.org/

23 Cap. 6.4.1

propria Certification Authority: i browser che l'includeranno non si accorgeranno di nulla.
Nel caso delle aziende, il loro obiettivo principale non è quello di certificare delle identità, ma di guadagnare rivendendo il servizio di certificazione. Ma verificare un'identità è costoso. Chi ci garantisce quindi che lo facciano correttamente? Che le loro chiavi private utilizzate per firmare siano conservate in modo sicuro[24]? Per l'ennesima volta è una questione di fiducia. Possiamo solo sperare che, non fosse per altro che per mantenere in piedi la loro attività, queste aziende di certificazione facciano bene il loro lavoro…
Se non fosse che… degli esempi mostrano che a volte il loro lavoro l'hanno fatto molto male.
Ad esempio, nel 2008 dei ricercatori sono riusciti a creare dei falsi certificati "validi" perché sei Certification Authority utilizzavano ancora degli algoritmi di cifratura deprecati dal 2004[25]. I certificati creati in questo modo sono dei "veri-falsi" certificati: il browser li riconosce come veri e, nonostante le loro origini fraudolente, tutto lascia pensare che siano stati rilasciati da un'autorità riconosciuta.
Nel 2011 sono stati creati nove veri-falsi certificati firmati da Comodo, una Certification Authority. Almeno uno di questi certificati sarebbe stato utilizzato nel web[26]. L'azienda ci ha messo più di una settimana per ammettere pubblicamente questa compromissione – e rimane il sospetto che molte aziende di questo tipo, trovandosi nella stessa situazione, non lo ammettano affatto, per evitare la pubblicità negativa[27] e le perdite economiche che ne deriverebbero.

---

24 Cap. 3.4.2
25 Alexander Sotirov, et Al., 2008, *MD5 considered harmful today – Creating a rogue CA certificate* [sepuzi.vado.li].
26 Comodo, 2011, *Comodo Fraud Incident* [duzisa.vado.li].
27 Jacob Appelbaum, 2011, *Detecting Certificate Authority compromises and web browser collusion* [putazu.vado.li].

Inoltre, sembra che a seguito di richieste da parte di polizia o autorità giudiziarie, alcune Certification Authority consegnino alle guardie dei veri-falsi certificati, creati al posto di quelli delle identità che vogliono sorvegliare[28].
Detto questo, qualora anche questi veri-falsi certificati fossero messi al posto giusto su internet, per essere sfruttati al meglio dovrebbero essere combinati con un attacco Man in the Middle[29]. Infine è bene ricordare che le nostre connessioni passano in generale attraverso diversi Paesi e che questo attacco può essere effettuato da un Paese differente rispetto a quello da cui ci connettiamo.
In una brochure commerciale, Packet Forensics, una compagnia americana che vende del materiale per la sorveglianza in rete, scrive che «per utilizzare il nostro prodotto in questo scenario, gli utilizzatori governativi hanno la possibilità di importare una copia di una chiave legittima che possono ottenere (potenzialmente grazie a un ordine della magistratura)»[30].
L'amministratore delegato di Packet Forensics avrebbe confermato a voce all'autore dello studio che clienti governativi collaborano con alcune autorità di certificazione per ottenere dei veri-falsi certificati da utilizzare nel corso delle operazioni di sorveglianza[31].

---

28 Christopher Soghoian, Sid Stamm, 2011, *Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [zafibu.vado.li].

29 Cap. 6.4.1

30 «To use our product in this scenario, government users have the ability to import a copy of any legitimate key they obtain (potentially by court order)». Citazione estratta dal paper di Christopher Soghoian et Sid Stamm, vedi sotto.

31 Questa citazione si trova in una versione preliminare, con data aprile 2010, del paper di Christopher Soghoian et Sid Stamm; questa versione è disponibile su cryptome.org [sapezu.vado.li].

### 6.4.3 Web of Trust

Un'altra possibile soluzione alla questione dell'autenticità delle chiavi pubbliche è il Web of Trust.
Piuttosto che fidarsi di una qualche autorità centralizzata, si stabilisce una catena di fiducia. Ovvero: Betty non conosce Alice, ma conosce invece Daniele, che conosce Emilia, che conosce Alice. C'è quindi un *percorso di conoscenze* che porta da Betty ad Alice. Anche questa catena di fiducia comporta che Betty debba fidarsi molto di Emilia, che però non conosce direttamente. Ma tra le conoscenze di Betty c'è anche Francesca, che conosce Gastone, che a sua volta conosce Alice e anche Heloise, che conosce Ingrid, che conosce anche lei Alice. In questo caso ci sono quindi tre catene di fiducia tra Alice e Betty, che, a questo punto, non ha bisogno di avere una fiducia completa in nessuna delle parti in gioco nella certificazione.
Questo tipo di metodo viene correntemente utilizzato per l'autenticazione dei programmi e delle comunicazioni personali, come caselle di posta che usano lo standard OpenPGP. Purtroppo non è invece utilizzato per autentificare siti web, anche se tecnicamente sarebbe possibile[32].
Il Web of Trust permette quindi di mettersi al riparo da attacchi Man in the Middle[33] senza doversi fidare di autorità centralizzate. Tuttavia necessita di rendere pubblici dei legami tra le identità, cosa che ha delle conseguenze non sempre auspicabili.

## 6.5 Forward Secrecy

Come abbiamo visto, chiunque possieda una chiave segreta

32 Il progetto Monkeysphere permette di estendere l'utilizzazione del Web of Trust di OpenPGP all'autenticazione dei siti web [web.monkeysphere.info].
33 Cap. 6.4.1

può utilizzarla per decifrare[34] un testo che è stato cifrato utilizzando la chiave pubblica ad essa associata. Si tratta di una funzione molto utile, ma che in certi casi può rivelarsi imbarazzante.
Poniamo che una persona mal intenzionata intercetti online una conversazione cifrata tra due persone. Sul momento non potrà leggerne il contenuto. Ma potrebbe volersi introdurre in seguito in casa di quelle persone, oppure voler accedere ai loro computer e mettere le mani sulle loro chiavi private. In questo caso sarà in grado di leggere, a posteriori, tutte le conversazioni passate di cui era entrata in possesso.
È questo il caso di qualche anno fa, quando gli amministratori del server *autistici.org* si resero conto che, nel corso di un'indagine, la polizia aveva messo le mani sulle chiavi segrete installate sui loro server, ottenendo così accesso al contenuto delle cartelle con scambi di email che altrimenti non sarebbe stata in grado di leggere[35].
Per evitare che un segreto non più segreto possa compromettere a posteriori molti altri segreti che dipendono da esso (come per esempio il contenuto di conversazioni cifrate svolte su instant messaging, scambi di email ecc.) alcuni programmi includono delle funzioni chiamate di "Perfect Forward Secrecy"[36].
Queste funzioni assicurano che anche se un giorno un segreto a lunga scadenza, tipicamente una chiave privata, venisse scoperto da un avversario, gli scambi sarebbero protetti contro un'analisi a posteriori.
In pratica, invece di utilizzare direttamente la chiave pubblica per cifrare le comunicazioni, questo tipo di cifratura usa un protocollo di scambio pensato per funzionare anche su un

34 Cap. 6
35 Autistici, 2005, *CRACKDOWN, violato autistici.org – Come ci hanno fregato* [merutu.vado.li].
36 Wikipedia, *Forward Secrecy.*

canale di comunicazione non sicuro, attraverso la negoziazione di una chiave temporanea all'inizio di ciascuna sessione di comunicazione. La chiave segreta in questo caso serve solo ad assicurare che stiamo comunicando con la persona giusta attraverso la firma di questa negoziazione.
È solo in un secondo momento che questo segreto temporaneo viene utilizzato per cifrare in modo simmetrico[37] le comunicazioni.
Una volta terminata la comunicazione, è sufficiente che i programmi implicati dimentichino questo segreto temporaneo. Anche se qualcuno mettesse le mani sulle chiavi segrete di entrambe le parti, l'intimità della comunicazione non sarebbe compromessa: neanche gli stessi partecipanti alla comunicazione potrebbero più accedervi.

## 6.6 Riepilogo e limiti

La crittografia asimmetrica è insomma un buon complemento alla crittografia simmetrica quando non si tratta di proteggere solo i nostri dati, ma anche il contenuto di una comunicazione: uno scambio di email, la navigazione web, delle conversazioni sull'instant messaging, ecc. Utilizzarla non è così complicato come si potrebbe pensare, e far diventare la cifratura un'abitudine permette a delle informazioni particolarmente sensibili di disperdersi nel mucchio di una grande mole di conversazioni cifrate.
Questa cifratura è particolarmente efficace quando è di tipo end-to-end, ovvero quando il mittente cifra il messaggio in modo che solo il destinatario finale lo possa decifrare.
Per concludere questo piccola panoramica delle tecniche crittografiche, è bene ricordare che la cifratura, per quanto diffi-

37 Tomo I, cap. 5.3

cile sia da rompere, ha sempre i limiti[38], che abbiamo evocato nel primo volume di questa guida. Questi limiti riguardano in particolare la fiducia che riponiamo nel computer e nei programmi a cui affidiamo le operazioni di cifratura e decifratura (a cui affidiamo, insomma, il testo in chiaro). E riguardano anche l'obbligo legale di fornire alle autorità il mezzo per decifrare le nostre comunicazioni, nel momento in cui ce lo chiedono[39]. Riguardano, infine, l'evoluzione della crittografia stessa: ciò che non è possibile fare oggi, potrebbe esserlo domani.
In ultimo va ricordato che, se la cifratura permette di nascondere il contenuto della comunicazione, le parti implicate (chi comunica con chi) restano evidenti.

38 Tomo I, cap. 5.1.4
39 Questo obbligo esiste in Francia, ma non in Italia [NdT].

# 7 | Anonimato nella comunicazione: l'onion routing

Utilizzare dei protocolli cifrati permette di ottenere una certa riservatezza su internet: un avversario non sa cosa ci stiamo dicendo. È facilmente in grado però di determinare la sorgente e la destinazione della comunicazione.
Vediamo adesso come e quanto possiamo provare a dissimulare da dove proviene e dove va una comunicazione.

## 7.1 Presentazione dell'onion routing

L'onion routing, utilizzato per esempio in Tor[1], può fornire un certo *anonimato* su internet mascherando da dove proviene una comunicazione. Utilizzando un sistema di questo tipo, l'indirizzo IP[2] che appare su internet, e che verrà registrato per esempio nei log di connessione dei server utilizzati, non è il nostro, ma quello di un altro computer.

### 7.1.1 Celare l'origine e la destinazione

Abbiamo visto che i pacchetti IP, come una cartolina postale, sono formati da diverse parti[3]. Da una parte il contenuto, specifico per ciascuna applicazione, che corrisponde ai dati che vogliamo effettivamente trasmettere: una email, una pagina web, dell'audio, ecc. Dall'altra parte le intestazioni, che contengono, tra le altre cose, indirizzo IP di origine e di destinazione, o

---

1 Gran parte di questo capitolo è ispirato al sito web di Tor: https://www.torproject.org/
2 Cap. 1.2.5
3 Cap. 1.2.3

anche la dimensione dei dati trasportati. Anche cifrando i dati, le intestazioni restano visibili. Esse rivelano al destinatario della comunicazione da quale macchina di internet proviene. Rivelano anche a tutti gli avversari che sorvegliano il traffico molte cose su chi siamo e cosa facciamo su internet.
Un classico problema riguardo l'anonimato è che il destinatario di una comunicazione può sapere chi è il mittente, guardando le intestazioni. Stessa cosa accade con gli intermediari autorizzati, come i provider internet, e a volte anche con quelli non autorizzati. Un tipo di analisi del traffico molto semplice consiste quindi, per esempio, nell'intercettare il traffico tra un mittente e un destinatario e guardarne le intestazioni.
La cifratura nasconde soltanto il contenuto del traffico, non le intestazioni. Non ci protegge quindi da questo tipo di attacchi. Inoltre esistono degli attacchi più complessi per trovare la sorgente e la destinazione di una comunicazione. Per esempio l'analisi del traffico di rete di cui abbiamo parlato precedentemente[4]: un avversario spia molti punti ben scelti di internet (per esempio, la connessione ADSL di Alice e il server che ospita un blog anonimo sul quale lei scrive) e fa la comparazione tra i pattern dei dati che transitano. L'avversario in questo modo è in grado di confermare se la comunicazione che sta sorvegliando provenga da una tale sorgente e vada verso una tale destinazione.

### 7.1.2 Una soluzione: una rete decentralizzata di anonimizzazione

Tor significa "The Onion Router", ovvero "routing a cipolla". Si tratta di un software libero[5] e di una rete pubblica che aiuta a ridurre le conseguenze di un'analisi del traffico di rete.

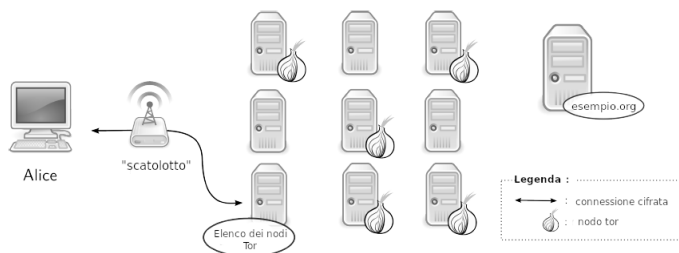
---

4 Cap. 3.4.3
5 Tomo I, cap. 4.1

Si fanno transitare le comunicazioni all'interno di una rete distribuita i cui nodi, chiamati "relay", sono ospitati da volontari sparsi in tutto il mondo. È come utilizzare un percorso tortuoso e difficile da seguire per seminare un inseguitore, cancellando le proprie tracce a ogni svolta. Invece di costruire un itinerario diretto tra la sorgente e il destinatario, i pacchetti di dati seguono un tragitto casuale attraverso vari nodi. Un avversario che osserva da un unico punto, non è quindi in grado di associare la sorgente e il destinatario.

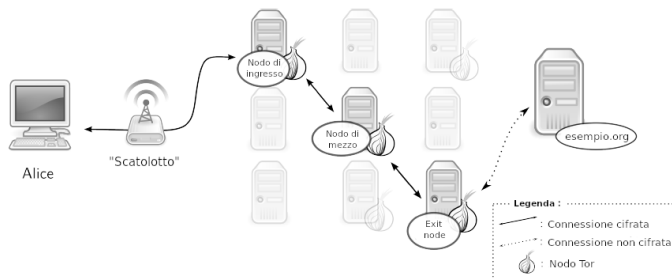
**Creazione di un circuito**

L'idea è che quando Alice vuole connettersi a esempio.org utilizzando Tor, il suo computer inizia come prima cosa a stabilire un circuito Tor.

Per farlo recupera una lista di nodi Tor disponibili all'interno di un elenco:

*Schema relay Tor*

In seguito sceglie un primo nodo tra quelli dell'elenco di nodi disponibili e stabilisce una connessione verso di esso. A partire da questo primo nodo viene stabilita una connessione verso un secondo nodo. Infine Tor sceglie dall'elenco un nodo di uscita (exit realy) e stabilisce una connessione tra il secondo e

quest'ultimo nodo. Questo insieme di tre nodi è quello che viene chiamato "circuito Tor". Dal momento in cui si stabilisce una connessione con questo circuito Tor, tutte le comunicazioni sono cifrate.

**Utilizzo del circuito**
Successivamente i dati transiteranno attraverso questi tre nodi prima di giungere al server di destinazione (esempio.org). La risposta del server seguirà lo stesso tragitto, in direzione opposta.

*Schema di utilizzo di un circuito Tor*

Il circuito viene percorso passo passo e ciascun nodo che si attraversa lungo il cammino non sa qual è quello che gli ha trasmesso i dati e quello a cui li ritrasmetterà. Nessun nodo da solo è in grado di conoscere il percorso completo intrapreso da un pacchetto di dati. Allo stesso modo, un eventuale intruso o un nodo compromesso non potrebbero analizzare facilmente il traffico di rete per stabilire una relazione tra la sorgente e il destinatario della connessione. Insomma, nessuno di questi può sapere che il computer di Alice si sta connettendo a esempio.org.

Avrete notato che un circuito Tor si compone di tre intermediari. Se venisse utilizzato un solo intermediario, basterebbe la sua compromissione[6] a mettere in pericolo il nostro anonimato, perché sarebbe a conoscenza sia dell'origine che della destinazione della comunicazione. Il fatto di utilizzare tre nodi permette di evitare questa raccolta di informazioni, senza rallentare eccessivamente la connessione.
Come precauzione ulteriore, il circuito Tor utilizzato non è sempre lo stesso, ma in un'ora cambia automaticamente diverse volte.

**Cifratura a cipolla**
Come abbiamo visto, il computer di Alice negozia una connessione cifrata con ciascun nodo del circuito utilizzato. In questo modo i dati che vuole trasmettere verso esempio.org conteranno molteplici *strati* di cifratura, come i veli di una cipolla. Il primo strato sarà cifrato in modo da poter essere letto solo dal terzo strato. Il secondo strato, sopra il primo, sarà leggibile solo al secondo nodo. Infine il terzo strato potrà essere letto solo dal primo nodo. Per questa ragione parliamo di "cifratura a cipolla". Ogni volta che passiamo per un nodo viene *aggiunto* un livello di cifratura. I singoli nodi potranno decifrare unicamente le informazioni che gli sono destinate.
Il terzo e ultimo nodo viene chiamato "exit realy": la connessione sembrerà provenire da lui, quindi sarà quello che rischierà di più di essere soggetto a controlli.

### 7.1.3 Gli Onion Service di Tor

Nel caso in cui degli utenti Tor vogliano fornire anche dei servizi, come per esempio un sito web o un server di instant

6 Cap. 3.4.2

messaging, hanno la possibilità di mascherarne la locazione geografica. Si tratta di ciò che viene chiamato Onion Service[7]. Come nel caso di ogni utilizzatore della rete Tor, l'indirizzo IP del server non viene mostrato. Inoltre, chi si vuole connettere a questo servizio dovrà necessariamente farlo attraverso la rete Tor. Gli Onion Service assicurano quindi un certo anonimato sia per chi gestisce i server sia per chi li utilizza. Questi Onion Service hanno degli indirizzi che finiscono con .onion.
Per collegarcisi, gli altri utenti Tor utilizzano il sistema dei "rendez-vous point" di Tor. Il "rendez-vous point" è il terzo nodo per ciascuno dei due protagonisti dello scambio: il client e il server. Il client costruisce un circuito Tor che abbia come terzo nodo questo "rendez-vous point". Dall'altra parte, il server dell'Onion Service farà la stessa cosa. A questo punto il client e il server possono "incontrarsi" e scambiarsi informazioni.
Questi Onion Service possono per esempio mettere online un sito web sul quale gli autori possano pubblicare senza essere censurati. L'indentificazione della locazione fisica del server che fornisce il sito web, così come quella dei suoi contributori e dei suoi visitatori, viene effettivamente resa molto più difficile che nel quadro di un sito web convenzionale: occorrerebbe mettere in atto un attacco alla rete Tor[8].

## 7.2 Partecipare alla rete Tor

La rete Tor appoggia su una base di volontariato ed è aperta a chiunque, poiché nessun nodo è in grado di conoscere la provenienza e la destinazione delle comunicazioni. A parte gli exit realy, nessun nodo può neanche conoscere il contenuto delle comunicazioni che sta trasportando. Quindi chiunque lo voglia può far girare su una macchina a sua scelta un nodo Tor.

7 The Tor Project, 2013, *Tor: Hidden Service Protocol* [zaduci.vado.li]
8 Cap. 7.3.4

Questo nodo verrà aggiunto alla rete Tor e veicolerà il traffico delle persone che lo utilizzano.

### 7.2.1 Configurare un nodo Tor

Il fatto che ciascun utente possa configurare un nodo, introduce della diversità rinforzando in questo modo l'efficacia della rete Tor nel suo insieme. Nonostante ciò, i nodi non sono tutti uguali rispetto all'attenzione che possono attirare. Se un nodo posto in prima o seconda posizione di un circuito Tor può non risultare troppo rischioso per Alice in Francia, un exit realy è invece più suscettibile di attirare l'attenzione verso la sua connessione. Eventuali avversari potrebbero interessarsi al suo nodo e magari andare a fare una perquisizione a casa sua, oppure sequestrarle il computer perché stanno conducendo un'inchiesta su qualcuno che è passato attraverso il suo exit realy per delle attività "sospette". Ovviamente è possibile configurare Tor in modo che il nostro nodo non sia utilizzato come exit realy, ma unicamente come primo o secondo nodo.
I nodi Tor legalmente sono considerati come dei router[9] e quindi Alice non è tenuta a conservare i log, ovvero di archiviare le tracce delle comunicazioni tra un IP e l'altro. Questo è un bene perché, anche se un singolo nodo preso da solo non sa un granché, se la rete Tor si ritrovasse a poco a poco composta in buona parte da nodi che conservano i log, sarebbe più facile ricostruire i circuiti a posteriori.

### 7.2.2 Configurare un bridge Tor

È anche molto utile mettere su dei "bridge" Tor. Si tratta di

9 Nos Oignons, 2013, *Qu'est-ce que c'est* [suzabi.vado.li].

nodi particolari che non sono elencati nelle liste pubbliche della rete Tor[10]. Servono a consentire l'accesso alla rete Tor anche a quegli utilizzatori che hanno l'accesso a internet filtrato verso le connessioni Tor.

## 7.3 Qualche limite di Tor

Come tutti gli strumenti di questo tipo, Tor può facilmente dare una falsa impressione di sicurezza e farci dimenticare che sta rispondendo a un problema circoscritto. Anche se effettivamente possiamo dire che risponda piuttosto bene al bisogno di dissimulare il proprio indirizzo IP e al bisogno di mascherare con quale server stiamo comunicando, non è comunque in grado di risolvere diversi altri problemi.
Come viene precisato sul sito di Tor[11], occorre sapere tre cose fondamentali prima di iniziare:

1. Tor non ci protegge se non lo stiamo utilizzando correttamente;
2. anche se l'abbiamo configurato e lo stiamo utilizzando correttamente, ci sono ancora dei possibili attacchi che possono compromettere la protezione fornita da Tor;
3. ora come ora nessun sistema di anonimizzazione è perfetto, e Tor non fa eccezione: sarebbe imprudente fare affidamento soltanto sulla rete Tor se abbiamo bisogno di un serio anonimato.

Adesso dettagliamo meglio qualcuno di questi limiti.

---

10 È possibile ottenere gli indirizzi dei bridge visitando il sito web https://bridges.torproject.org/
11 https://www.torproject.org/

### 7.3.1 L'utente male informato o poco attento

Come spesso accade, quando siamo male informati, corriamo molti rischi di farci male. Quando utilizziamo uno strumento, in particolare se lo utilizziamo per proteggere la nostra vita privata, è molto importante capire bene a cosa serve, ma anche e soprattutto a cosa non serve, così come anche i suoi vari limiti.
Se Alice utilizza regolarmente Tor per consultare dei siti web potenzialmente pregiudizievoli nel suo paese, e allo stesso tempo sta anche leggendo le proprie email, un avversario potrebbe mettere in relazione i log del server[12] che ospita la sua casella di posta con quelli dei siti web che ha visitato. È probabile che in questo modo queste diverse connessioni appaiano come provenienti dallo stesso exit realy. Se si mettono in relazione anche le ore in cui ci si è collegati, è possibile aumentare ulteriormente le possibilità di individuazione.
In questo esempio, Alice utilizza differenti identità contestuali[13] in contemporanea e non può pretendere che Tor le sappia separare magicamente. Per evitare questo raggruppamento, la soluzione dovrebbe essere quella di cercare di compartimentare[14] le identità contestuali.

### 7.3.2 L'avversario vede che usiamo Tor[15]

Il fornitore di accesso a internet, o l'amministratore della rete locale di Alice può molto facilmente sapere che lei si sta connettendo a un nodo Tor, invece che a un server web ordinario.

12 Cap. 2.4
13 Cap. 5.2
14 Cap. 5.3
15 Questa sezione, come quelle seguenti, sono fortemente ispirate al sito web di Tails: https://tails.boum.org/

In effetti, l'indirizzo IP del server verso il quale il computer di Alice si connette sarà quello di un nodo d'ingresso alla rete Tor e l'elenco dei nodi d'ingresso è disponibile pubblicamente su internet.
Allo stesso modo il server di destinazione al quale si connette via Tor può sapere se queste comunicazioni provengono da un exit realy Tor.
Mentre sta usando Tor insomma, Alice non assomiglia a un'ordinaria utente internet. L'anonimato fornito da Tor funziona provando a mettere tutti i suoi utenti nello stesso cesto, in modo che non sia possibile distinguerli l'uno dall'altro. Più gente utilizzerà Tor e più varie saranno le loro attività, meno l'uso di Tor sarà sospetto. La solidità di questo strumento si poggia soprattutto su questo insieme non distinguibile di utenti, quello che inglese viene chiamato "anonymity set".

### 7.3.3 Gli exit realy Tor possono spiare le comunicazioni che transitano da loro

Se è vero che Tor impedisce di sapere dove ci troviamo, non cifra però le comunicazioni al di fuori della propria rete. Tor non può quindi cifrare ciò che transita tra gli exit realy e il server di destinazione. Ogni exit realy ha quindi la possibilità di catturare il traffico che passa tramite di esso.
Per esempio, nel 2007 un ricercatore in sicurezza informatica ha intercettato migliaia di email private inviate da ambasciate straniere e ONG attraverso il mondo. Ha utilizzato un attacco Man in the Middle[16] ed è riuscito ad ascoltare il traffico in uscita dall'exit realy che amministrava[17].
Per proteggersi da questi attacchi è necessario utilizzare la

---

16 Cap. 6.4.1
17 Kim Zetter, 2007, *Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise* [teniti.vado.li].

crittografia end-to-end, di cui abbiamo parlato nella parte precedente[18].

### 7.3.4 Timing attack

Per com'è concepito, Tor non permette di proteggersi da alcuni tipi di attacco, soprattutto quelli che riguardano l'analisi del traffico[19]. Il timing attack è uno di questi. L'idea dietro a questo attacco è quella di osservare il ritmo di invio dei dati in due punti del loro tragitto, per esempio sul primo nodo e sul terzo (l'exit realy). Inviamo per esempio un flusso come fosse un codice morse: 3 pacchetti inviati, poi 5 secondi di silenzio, poi altri 3 pacchetti, ecc.
Un avversario che vede che il computer di Alice invia al primo nodo un flusso con un dato pattern temporale e che osserva un flusso con lo stesso pattern sull'exit realy che va verso esempio.org, può dedurne che probabilmente chi si sta connettendo a esempio.org è il computer di Alice[20].
La forza, ma anche la fragilità di Tor, è che chiunque può possedere un nodo Tor: Alice, Betty, un'università, la CIA, ecc. Se un avversario ha le informazioni che riguardano un solo nodo dal quale transitano i dati, non ci sono problemi. Ma se malauguratamente degli avversari riuscissero a mettere le mani su più di un nodo, potrebbero costruire un timing attack.
I fornitori di accesso a internet e i grandi servizi di contenuti o di risorse utilizzati su molti siti web – inserti pubblicitari, funzionalità di ricerca e social sharing – si trovano in una buona posizione per osservare il traffico e collaborare a questo tipo di attacco.

---

18 Cap. 6
19 Wikipedia, *Analisi del traffico radio.*
20 Wikipedia, *Tor (software).*

### 7.3.5 Tor non protegge dagli attacchi confermativi

Abbiamo visto che, per com'è concepito, Tor non permette di proteggersi contro un attacco capace di misurare il traffico in entrata e uscita dalla rete Tor. Quando l'avversario è in grado di confrontare i due flussi, può metterli in relazione attraverso delle semplici statistiche.
Consideriamo adesso un avversario che abbia delle ragioni per pensare che sia Alice a pubblicare su un certo blog anonimo. Per confermare questa ipotesi, potrà mettersi a osservare il traffico che esce dalla connessione ADSL di Alice e quella che entra sul server che ospita il blog. Se confrontando i due flussi di traffico osserva gli stessi pattern di dati, avrà confermato la propria ipotesi.
Tor protegge Alice da un attaccante che voglia scoprire chi pubblica sul blog anonimo. Ma non protegge da un avversario che debba solo confermare un'ipotesi e che abbia i mezzi per farlo.
Questo tipo di attacco può anche essere effettuato con degli insiemi ipotetici più larghi: consideriamo un avversario che abbia identificato un gruppo di connessioni ADSL che gli interessano, e un server a cui sa che accedono. Se l'attaccante è in grado di accedere al traffico del gruppo in questione e a quello del server, per esempio grazie a una richiesta legale, mettendo insieme questa ipotesi e un timing attack, potrebbe trovare qual è la connessione all'interno del gruppo che si sta connettendo al server.
In questo modo un post su un server che ospita un blog può essere messo in relazione a una connessione specifica all'interno di un gruppo di persone sospettate di partecipare a quel blog anonimo.

### 7.3.6 Tor non protegge da un avversario globale

Infine, un caso particolare è l'avversario globale passivo. Per avversario globale passivo si intende una persona o un ente capace di guardare e quindi confrontare il traffico che transita tra tutti i computer di una rete. Studiando per esempio i volumi di informazioni delle differenti comunicazioni in ogni istante attraverso questa rete, sarebbe statisticamente possibile identificare un circuito Tor poiché ci sarebbe uno stesso flusso di informazioni che apparirebbe con un intervallo di qualche millisecondo su ciascun nodo del circuito. L'avversario potrebbe così collegare un utente Tor e il proprio server di destinazione.
Un avversario globale, che abbia dei mezzi paragonabili a quelli dell'NSA per esempio, potrebbe mettere in atto anche altri attacchi volti a rompere l'anonimato fornito dalla rete Tor. Tuttavia, non rispondere a una simile minaccia fa parte dei compromessi di Tor per consentire una navigazione ragionevole in termine di tempi di attesa quando per esempio si naviga sul web o si usa l'instant messaging[21].
Malgrado tutto, i rischi che derivano da questi limiti non sono paragonabili a quelli a cui andiamo incontro navigando in modo non-anonimo. Tor è uno degli strumenti più efficaci in materia di anonimato su internet e, se li teniamo a mente, questi rischi non devono dissuaderci da un suo utilizzo consapevole.

21 Roger Dingledine, Nick Mathewson, Paul Syverson, 2004, *Tor Project: The Second-Generation Onion Router* [cazoco.vado.li].

SECONDA PARTE

# Scegliere le risposte adatte

Ci prende di nuovo il panico. Tutto ciò che facciamo online ci tradisce, giorno dopo giorno. E pensare che credevamo, a torto, di “essere in sicurezza”...
Ma prima di tornare al piccione viaggiatore e alla lettera sigillata e scritta in codice – soluzioni dal sapore antico ma, ricordiamolo, sempre efficaci – abbiamo ancora un po’ di margine di manovra. Non moltissimo, ma qualcosa sì.
Ancora una volta, sarà proprio questo margine che andremo ad analizzare.
All’interno di questa parte, descriveremo alcune situazioni tipiche, che chiameremo “casi d’impiego”, in modo da illustrare le nostre proposte.

# 8 | Caso d'impiego: navigare dei siti web

## 8.1 Contesto

Quello che ci interessa ora è la consultazione delle informazioni disponibili sul web: leggere un giornale, seguire un blog, ecc. Attività del tutto normali mentre siamo online.
Però vogliamo effettuare queste attività in modo discreto, per varie ragioni, tra le quali possiamo citare:
• sviare il controllo o evitare la censura, quella di un padrone, di un vicino o di uno Stato;
• evitare la profilazione e la raccolta dei dati personali a fini commerciali.

## 8.2 Valutare i rischi

Questo problema è così vasto e complesso che è difficile capire bene da che parte approcciarlo. Dividiamolo quindi in pezzi.

### 8.2.1 Cosa vogliamo proteggere?

In questo caso d'impiego, ciò che ci interessa difendere in primo luogo è l'anonimato, o quantomeno lo pseudonimato: quello che cerchiamo di nascondere non è il *contenuto* di ciò che stiamo consultando, ma *il fatto che siamo noi a consultarlo*.
Abbiamo visto in precedenza che l'utilizzo di internet, in particolare del web, lascia numerose tracce, di diversa natura e in diverse direzioni; molte di queste, come tante briciole, tracciano un percorso che porta dalla risorsa consultata fino a una casa, a un preciso computer, e quindi a una persona che ci sta dietro. Sono queste tracce in rete, prime fra tutte quelle che

contengono l'indirizzo IP[1], ciò di cui ci vogliamo sbarazzare. Essendo però l'indirizzo IP necessario al buon funzionamento della rete, la strategia sarà quella di fare in modo che i curiosi che vorranno seguire questa pista si ritrovino in un vicolo cieco. Inoltre potremmo eventualmente voler non lasciare alcuna traccia della nostra navigazione sul computer utilizzato, in particolare sul suo hard-disk.

### 8.2.2 Da chi vogliamo proteggerci?

Questa è una domanda importante: a seconda della risposta, la policy di sicurezza adeguata può cambiare notevolmente.

**Fornitori di accesso a internet**
Alice lavora per una grande ditta e accede a internet attraverso la rete aziendale. Guarda i suoi blog preferiti durante l'orario di lavoro, ma non vuole che il datore di lavoro lo sappia. In questo caso Alice ha bisogno di proteggersi dallo sguardo indiscreto del tecnico amministratore di sistema, incaricato dall'azienda. In questo caso l'avversario ha accesso all'insieme del traffico di rete che transita attraverso la propria connessione e sul quale ha il ruolo di postino. In compenso, non possiede altri occhi in altri punti strategici di internet.

**Fornitori di contenuti**
Betty è iscritta a un forum della polizia, e passa il tempo – non senza un certo malizioso piacere – a seminare zizzania nelle discussioni delle guardie. In questo caso, Betty non vuole rendere noto al sito che ospita il forum che è lei l'autrice dei disturbi. Come abbiamo visto, il suo indirizzo IP verrà conservato per più o meno tempo dal sito visitato[2]. In questo caso

1 Cap. 1.2.5
2 Cap. 3.2.2

l'avversario avrà accesso agli header IP[3] e HTTP[4] poiché ne è il destinatario.

**Avversari diversi e molteplici**
Agata visita regolarmente il sito di pubblicazione di documenti confidenziali sul quale Benoît ha pubblicato degli estratti conti bancari[5]. Trattandosi di un argomento sensibile, lei sa in partenza che il blog in questione potrebbe essere sorvegliato. Quindi non vuole che nessuno sappia che lo sta consultando.
In questo caso non sappiamo dove l'avversario[6] potrebbe posizionare il suo sguardo: può metterlo al livello del computer di Agata, a quello del suo router, al livello del blog oppure in un qualsiasi altro posto sul tragitto[7] tra il computer e il blog. L'avversario potrebbe anche posizionarsi in più luoghi contemporaneamente.

## 8.3 Definire una policy di sicurezza

Adesso poniamoci le domande consuete del nostro metodo[8]:

1. Quale insieme di pratiche e strumenti ci proteggerebbe in modo sufficiente contro i nostri avversari?
2. Di fronte a una policy di sicurezza di questo tipo, quali sarebbero le strategie d'attacco più praticabili?
3. Quali mezzi sarebbero necessari per sbaragliarla?
4. Pensiamo che i nostri avversari abbiano a disposizione questi mezzi?

---

3 Cap. 1.2.5
4 Cap. 2.4.1
5 Cap. 0 (Prefazione)
6 Precisiamo che qui, a differenza del caso precedente, crediamo che l'avversario non sia il gestore del sito (o solo di esso), ma un altro soggetto; e quindi dobbiamo capire cosa questo soggetto potrebbe fare [NdT].
7 Cap. 1.4.3
8 Tomo I, cap. 7

### 8.3.1 Prima strategia: chiedere a chi vede

*Tipo di attacco più praticabile dall'avversario*: analizzare i dati salvati dal server[9] che ospita le risorse consultate.
*Mezzi necessari*: potersi connettere al server che fornisce la connessione (nel caso in cui l'avversario sia il fornitore di accesso a internet, o collabori con lui); o potersi connettere al server che ospita la risorsa (se l'avversario è il fornitore del contenuto o un suo collaboratore).
Se l'avversario è il fornitore d'accesso a internet o il fornitore del contenuto, gli basterà consultare i propri log[10] delle connessioni. Ma anche per altri avversari è possibile accedere a queste informazioni, per mezzo di una richiesta legale[11], di un contratto commerciale, di una collaborazione volontaria[12], o anche di un'intrusione[13].
*Plausibilità di un simile attacco*: probabile se la nostra connessione o il sito stesso attira l'attenzione dell'avversario.
Contro questo tipo di attacco, una soluzione efficace è quella di utilizzare il routing a cipolla[14][15] servendosi della rete Tor nel modo di cui parleremo in seguito. Per assicurarsi il massimo dell'anonimato sarà poi necessario non mischiare le proprie attività quotidiane normali con quelle che vogliamo restino più discrete, in modo da non creare collegamenti tra le nostre

---

9 Cap. 3.2
10 Cap. 3.2
11 Cap. 3.2.4
12 Jacques Follorou, 2014, *Espionnage: comment Orange et les services secrets coopèrent*, Le Monde [fegabo.vado.li].
13 Cap. 3.4.2
14 Cap. 7
15 Contro alcuni degli avversari elencati, possono bastare delle soluzioni tecniche meno potenti di quelle che offre Tor. L'utilizzo di una VPN, per esempio. Nonostante ciò, nel più ci sta il meno, e Tor protegge da più attacchi rispetto a una VPN, che invece frappone un solo intermediario tra noi e la risorsa consultata. Cfr. Wikipedia, *VPN*.

diverse identità contestuali[16].

### 8.3.2 Seconda strategia: guardare sul computer utilizzato

Finché utilizziamo Tor, l'avversario che osserva i dati che circolano sulla rete non può sapere né da dove vengono né dove vanno e deve quindi trovare un altro modo per scoprirlo.
*Tipo di attacco più praticabile*: accedere alle tracce[17] lasciate sul computer dai siti visitati.
*Mezzi necessari*: accesso al computer utilizzato.
*Plausibilità*: nel caso di Alice che utilizza il computer dal suo ufficio, è molto facile per il suo avversario. Negli altri casi e a seconda dell'avversario, è necessario un sequestro (che quando è legale viene chiamato anche perquisizione), o di attaccare il computer installandogli sopra un software malevolo[18].
Per difendersi è necessario cifrare il proprio hard-disk[19] in modo da rendere difficile l'accesso alle tracce lasciate. Oppure, meglio ancora, evitare in partenza di lasciare tracce del tutto: utilizzando un sistema live amnesico[20], che non salverà niente sul computer che si utilizza.

### 8.3.3 Terza strategia: attaccare Tor

*Tipo di attacco*: sfruttare i limiti dell'anonimato forniti da Tor[21], per esempio effettuando un attacco per conferma[22].

---

16 Cap. 7
17 Tomo I, cap. 2
18 Tomo I, cap. 3
19 Tomo I, cap. 15
20 Tomo I, cap. 14
21 Cap. 7.3
22 Cap. 7.3.5

*Mezzi necessari*: bisogna essere in grado di sorvegliare diversi punti nella rete, per esempio la connessione utilizzata *e* il sito consultato.
*Plausibilità*: un avversario, come potrebbe essere un'azienda che cerca di sorvegliare i propri dipendenti, ha poche possibilità di mettere in piedi un attacco del genere. Lo stesso vale per il commissariato di Saint-Tropez. Può però essere alla portata di un fornitore di servizi a livello nazionale o mondiale, o di guardie specializzate. Ancora una volta, non dimentichiamo che c'è una grande differenza tra avere la capacità tecnica di mettere in atto un attacco e farlo per davvero. Questa differenza tiene conto, per esempio, del rapporto tra i costi economici e i benefici dell'investimento.
Ricordiamoci inoltre di quando abbiamo parlato del fatto che molti altri attacchi contro Tor sono possibili o temibili. È importante capire bene gli obiettivi[23] e i limiti[24] di Tor per evitare di tirarsi la zappa sui piedi.

## 8.4 Scegliere tra gli strumenti disponibili

Dovremo scegliere tra i diversi strumenti in base ai nostri bisogni e alla nostra policy di sicurezza.

### 8.4.1 Il Tor Browser sul nostro sistema o dentro Tails

#### Il Tor Browser sul nostro sistema operativo

Configurare un browser web per utilizzare Tor correttamente è un esercizio difficile. È soprattutto per venire incontro a questa difficoltà che esiste il Tor Browser. Il Tor Browser è una suite di software: ci offre un browser web preconfigurato

23 Cap. 7.1.1
24 Cap. 7.3

per navigare in modo anonimo, utilizzando la rete Tor, a partire dal nostro sistema operativo abituale[25]. Una volta installato[26] il Tor Browser, possiamo scegliere di utilizzare questo browser oppure il nostro solito.

*Vantaggi*: il Tor Browser permette di navigare sul web con Tor all'interno del nostro sistema operativo abituale. Permette per esempio di lavorare su un documento con i nostri soliti strumenti, cercando informazioni in modo anonimo.

*Inconvenienti*: il Tor Browser eseguito sul sistema operativo comporta una falla attraverso la quale un avversario potrebbe limitare la protezione offerta dalla rete Tor. Ma soprattutto, utilizzata all'interno di un sistema non amnesico, il Tor Browser lascerà probabilmente delle tracce sull'hard-disk del computer utilizzato.

Gli aggiornamenti di Firefox, sul quale il Tor Browser è basato, possono avere dei tempi di rilascio più o meno lunghi rispetto a quelli del Tor Browser stesso. Nell'arco di questo tempo potrebbe presentare delle falle di sicurezza note e rese pubbliche

[NdT: *Negli ultimi anni questo problema è stato corretto: i rilasci di Firefox, Tor Browser e Tails avvengono ora in maniera sincronizzata*].

Infine, con le impostazioni di default, d'altra parte modificabili, potrebbe succedere di perdere tutte le finestre aperte e le ricerche in corso, se per esempio il Tor Browser si piantasse all'improvviso.

D'altro canto, il Tor Browser non impedisce ad altri programmi di connettersi a internet senza passare da Tor, anche se vengono aperti partendo da link trovati con il Tor Browser (programmi P2P, lettori pdf, visualizzatori di file multimediali, ecc.).

---

25 Nel nostro caso si tratta di Debian, ma il Tor Browser funziona anche con tutte le altre distribuzioni GNU/Linux, e anche con Windows o Mac OS.

26 Cap. 13

**Tails**

Tails[27] è un sistema *live*[28] il cui scopo è quello di preservare la riservatezza e l'anonimato dei propri utenti. Permette di utilizzare internet in modo anonimo quasi da qualsiasi posizione e computer. Inoltre non lascia alcuna traccia sul computer delle attività effettuate, a meno che non lo si chieda esplicitamente.
*Vantaggi*: utilizzando Tails, non solo non lasciamo tracce sul computer, ma i programmi che hanno bisogno di accedere a internet sono configurati per passare attraverso la rete Tor, e le connessioni dirette (che non permettono l'anonimato) sono bloccate.
Inoltre, siccome si tratta di un sistema live, Tails si avvia a partire da un DVD o da una penna USB, senza modificare il sistema operativo installato sul computer. Può quindi essere utilizzato sia a casa che da un amico, o nella biblioteca di quartiere.
Per avere più informazioni, consultate la pagina "A proposito" di Tails[29].
*Inconvenienti*: Prima di tutto, essendo Tails un sistema operativo[30] a sé stante, per utilizzarlo è necessario riavviare il computer[31]. È anche più complesso da installare rispetto al Tor Browser. Infine è necessario avere con sé una penna USB (di almeno 8 GB ) oppure un DVD che contenga Tails.
Inoltre, proprio a causa del sistema amnesico, se per caso il

27 Tomo I, cap. 14
28 https://tails.boum.org/
29 luveza.vado.li
30 Tomo I, cap. 1.4.1
31 Possiamo anche utilizzare Tails all'interno di una macchina virtuale [tomo I, cap. 22], dentro il sistema che usiamo abitualmente. In questo caso la memoria della macchina virtuale sarà visibile dal sistema e tutti i dati utilizzati, password comprese, saranno vulnerabili alle falle di programmazione o a un eventuale software malevolo. Inoltre, se questo sistema utilizza la swap [tomo I, cap. 1.5.4], è possibile che alcuni dati della macchina virtuale finiscano per essere scritti sull'hard-disk. In questo modo il sistema amnesico di Tails è quasi impossibile da garantire.

browser dovesse piantarsi, perderemmo tutte le pagine che stavamo consultando, esattamente come nel caso del Tor Browser.
Per non mischiare le proprie attività quotidiane normali con quelle che vogliamo siano più discrete e per le quali quindi usiamo Tails, è necessario riavviare la macchina quando si passa da un'identità contestuale all'altra.

### 8.4.2 Fare la propria scelta

In fin dei conti dobbiamo scegliere tra:
- utilizzare il proprio sistema operativo abituale;
- utilizzare un sistema live amnesico

In altri termini, quali tracce (eventualmente cifrate) siamo disposti a lasciare sul computer o sulla penna USB che stiamo usando? Abbiamo bisogno del resto del nostro ambiente di lavoro durante la navigazione anonima?
Ancora una volta, non ci sono risposte giuste o sbagliate: si tratta di scegliere la soluzione che ci conviene di più. E possiamo anche provare una soluzione e poi passare all'altra se necessario.
Alla fine, le due possibilità che abbiamo sono:
- utilizzare il Tor Browser all'interno di una Debian cifrata[32]. Questo permette di navigare in modo anonimo utilizzando al tempo stesso il proprio sistema abituale. Di contro, lasceremo probabilmente alcune tracce (cifrate) sull'hard-disk;
- utilizzare il browser di Tails. Non lasceremo tracce sull'hard-disk né altrove a meno di non usare la persistenza[33].

Una volta fatta la nostra scelta, consultiamo qui di seguito il paragrafo corrispondente.

32 Tomo I, cap. 15
33 Tomo I, cap. 14.5

## 8.5 Navigare con il Tor Browser

Se, valutati i pro e i contro, decidiamo di utilizzare il Tor Browser invece che Tails, è bene prendere alcune precauzioni.

### 8.5.1 Fare la propria scelta

Prima di tutto, siccome non stiamo usando un sistema live, lasceremo delle tracce di navigazione sul nostro hard-disk (cookie, file scaricati..). Un buon inizio è applicare la stessa policy di Una nuova partenza[34]. A questo punto possiamo scaricare e installare il Tor Browser correttamente. Il capitolo che spiega come installarlo[35] descrive questa procedura.

### 8.5.2 Usare il Tor Browser

Nelle pagine che riguardano l'installazione del Tor Browser[36], viene anche spiegato come usarlo. Questo strumento è pensato per essere il più facile possibile da utilizzare. Al momento dell'avvio tutti i programmi di cui abbiamo bisogno (Tor e il browser Firefox) vengono lanciati e configurati. Bisogna quindi aspettare che la finestra di Firefox si apra e a quel punto potremmo cominciare la navigazione attraverso la rete Tor.

⚠ *Attenzione*: solo la consultazione dei siti attraverso questa finestra garantisce una connessione anonimizzata. Tutte le vostre altre attività (client mail, instant messaging, Torrent, ecc.) mostreranno il vostro vero indirizzo IP[37].

34 Tomo I, cap. 8
35 Cap. 13
36 Cap.13
37 Cap. 1.2.5

### 8.5.3 Ci si accorge presto dei limiti

Il Tor Browser è uno strumento molto utile per il suo utilizzo semplificato, ma se ne scoprono presto i limiti. In effetti, soltanto le connessioni partite con il Tor Browser passano per la rete Tor. Se vogliamo utilizzare un altro browser, la connessione passerà altrove, il che può trarre in inganno. Se non facciamo attenzione potremmo confondere il browser e pensare che la nostra navigazione stia passando ancora per la rete Tor, quando invece non è così. Inoltre in questo modo non è possibile utilizzare Tor per niente di diverso dalla navigazione web che, per quanto grande, è solo una parte di internet[38].
Aggiungiamo che l'anonimato di una connessione non consiste soltanto nel nascondere l'indirizzo IP. Tutte le tracce che lasciamo sul web e sul nostro computer potrebbero un giorno o l'altro tradirci e il Tor Browser non potrebbe proteggerci.
Infine, con il Tor Browser, è più facile finire col mischiare le identità contestuali, tanto più se viene utilizzato nello stesso ambiente dell'identità principale.

## 8.6 Navigare con Tails

### 8.6.1 Ottenere e installare Tails

Tails è un software libero, può quindi essere scaricato, usato e condiviso senza restrizioni[39]. Funziona su un computer indipendentemente dal sistema operativo installato. In realtà Tails viene lanciato da un supporto esterno, senza utilizzare l'hard-disk: bastano un DVD o una penna USB.
Dovremo come prima cosa scaricare Tails[40]. Per assicurarsi

38 Cap. 1.2.3
39 Cap. 4.1
40 Tomo I, cap. 14.2.1

che il download sia andato a buon fine, dovremo poi verificare l'immagine[41].Una volta effettuata la verifica, possiamo procedere all'installazione su una penna USB o un DVD[42].

### 8.6.2 Avviare Tails

Adesso che abbiamo installato Tails[43], lanciamolo. Potremo a questo punto cominciare a utilizzarlo senza alterare il sistema operativo presente sul computer.

### 8.6.3 Connettersi a internet

Una volta finito l'avvio di Tails, ossia una volta che si visualizza completamente il Desktop, ci resta solo da seguire il wizard di connessione[44] [45]. A questo punto possiamo navigare sul web.

### 8.6.4 Limiti

Una soluzione del genere si appoggia sull'utilizzo di Tor e di Tails e risente quindi dei limiti di entrambi questi strumenti:
Riguardo ai limiti di Tor, ne abbiamo parlato in precedenza[46].
Per quanto riguarda i limiti di Tails, troverete un elenco approfondito di avvertenze sul sito web del progetto[47].
Non possiamo far altro che invitarvi a leggere e rileggere attentamente questi due testi.

---

41 Tomo I, cap. 14.2.2
42 Tomo I, cap. 14.2.3
43 Tomo I, cap. 14.4
44 Sito di Tails: serina.vado.li
45 Cap. 14
46 Cap. 8.3.3
47 Sito di Tails: tugava.vado.li

# 9 | Caso d'impiego: pubblicare un documento

## 9.1 Contesto

Dopo aver finito la stesura di un documento sensibile[1], vorremmo pubblicarlo su internet preservando però il nostro anonimato (il documento non deve essere associato a nessun nome) o il nostro pseudonimato (il documento può venire associato soltanto a un nostro pseudonimo, diverso dal nome civile).
In più, vorremmo poter includere un indirizzo di contatto pubblico corrispondente a questo pseudonimo.

## 9.2 Valutare i rischi

### 9.2.1 Cosa vogliamo proteggere?

Il contenuto del documento è pubblico. In questo caso quindi non ci interessa la confidenzialità. Vorremmo invece mantenere nascosti i collegamenti tra il documento e le persone che l'hanno scritto. Quello che ci interessa è insomma l'*anonimato* o lo *pseudonimato*.

### 9.2.2 Da chi vogliamo proteggerci?

Come nel caso d'impiego precedente[2], proveremo a proteggerci dagli sguardi indiscreti che cercano di sapere chi fa cosa sul web. Tanto più pensiamo che il documento che stiamo per pubblicare possa indispettire persone in grado di nuocerci, quanto più dovremo prestare particolare attenzione alle

1 Tomo I, cap. 9
2 Cap. 8

tracce lasciate. In quel caso è possibile che si avvii un'indagine per tentare di risalire all'autore o agli autori del documento, tramite ad esempio delle richieste legali[3] ai provider[4].

## 9.3 Definire una policy di sicurezza

Vedremo per prima cosa come pubblicare i documenti e successivamente come adoperare un contatto pubblico collegato ad essi.

### 9.3.1 Pubblicazione

Pubblicare un documento significa tecnicamente salvarlo su un server[5] connesso ad internet, che chiameremo "host". Per realizzare questa operazione in genere si ricorre a un sito web. Però probabilmente sceglieremo siti diversi a seconda che si voglia pubblicare un testo, un audio o un video.
Si tratta quindi di scegliere il nostro host sapendo che i criteri di valutazione sono molteplici: tipo di documento, disponibilità, condizioni di hosting, resistenza dell'host alle pressioni giudiziarie, rischi che il nostro documento gli farà correre, ecc. Nella parte Utensili troverete una lista più esaustiva di questi criteri[6].
Una volta effettuata questa scelta, dobbiamo accertarci che il nostro documento resti consultabile: se per esempio la nostra pubblicazione non piacesse al nostro host, o se messo sotto pressione, magari con una richiesta legale, ne eseguisse la rimozione, la nostra opera potrebbe diventare irreperibile.

---

3 Cap. 3.2.4
4 Cap. 1.5
5 Cap. 1.5
6 Cap. 15

Per evitare questo tipo di disagi, possiamo moltiplicare i luoghi dove appoggiare il file, possibilmente in server situati in Paesi differenti. Considerando che i tempi di un'azione legale sono molto più lenti rispetto a quelli che ci vogliono per pubblicare un file online, questa può essere una valida soluzione per evitare la censura.
Quali saranno allora le strategie alla portata di un nostro eventuale avversario?

### 9.3.2 Prima strategia d'attacco: sta scritto in basso a sinistra

L'avversario dispone innanzitutto di una grossa mole di dati nella quale cercare indizi: il contenuto stesso del documento. Un'eventuale firma come pseudonimo, una città, una data, la lingua con cui è scritto il documento, o anche semplicemente il tema stesso del documento, sono tutti indizi che possono condurre ai suoi autori. Un testo che nel novembre 2012 descrive la condotta illegittima dell'azienda Machinex sarà stato scritto probabilmente da degli impiegati di questa azienda o da persone che hanno condiviso la loro lotta in quella data.
L'avversario può anche tentare un'analisi stilometrica[7] per confrontarlo con altri testi, anonimi o no, e provare a dedurne informazioni sugli autori. Per quel che sappiamo, questo tipo di strategia è veramente efficace solo quando si hanno già dei forti sospetti su un ristretto insieme di potenziali autori, ma si tratta di un campo di ricerca recente. Del resto, visto che vogliamo diffondere largamente questo documento, non potremo mascherarne il contenuto. Nonostante ciò, se pensiamo che ne valga la pena, possiamo provare a dedicare un'attenzione particolare nel cambiare il proprio stile di scrittura.

---

7 Cap. 5.2

Infine, se abbiamo pubblicato il nostro documento senza prendere precauzioni più ampie, un avversario potrebbe cercare eventuali metadati[8] che gli forniscano qualche informazione.
Questi vari metodi non richiedono particolari competenze tecniche e sono quindi alla portata di molti avversari.
Per proteggersi, seguiremo le seguenti ricette:

- se possibile, lavoreremo al nostro documento utilizzando fin da subito dei metodi[9] che limitano i metadati;
- in ogni caso, sarà bene eliminare eventuali metadati[10] prima della pubblicazione.

### 9.3.3 Seconda strategia d'attacco: chiedere a chi vede

In assenza di indizi facilmente deducibili dal documento, una delle strategie più praticabili è quella di cercare le tracce della sua pubblicazione in rete.
A seconda dei suoi mezzi, il nostro avversario può effettuare una richiesta legale [11]al servizio che ospita il contenuto oppure trovare un altro modo di procurarsi i log[12] di connessione e di conseguenza ottenere l'indirizzo IP utilizzato. In seguito può rivolgersi all'ISP (Internet Service Provider)[13] corrispondente a questo indirizzo IP per avere il nome dell'abbonato.
Anche in questo caso, per far fronte a questa minaccia, possiamo utilizzare Tor per connetterci a internet, confondendo così il percorso che porta alla pubblicazione.
Quanto alla scelta del servizio su cui ospitare il documento, sono sempre valide le considerazioni riportate sopra. In più, va

8 Cap. 2.6
9 Tomo I, cap. 9
10 Tomo I, cap. 24
11 Cap. 3.2.4
12 Cap. 3.2.2
13 Cap. 3.2.3

tenuto conto che alcune piattaforme non funzionano nel caso in cui si utilizzi Tor, e che usare alcune tecnologie come Flash[14] è fortemente sconsigliato se vogliamo mantenere l'anonimato: questo restringe di molto il campo dei servizi utilizzabili.
Per pubblicare il nostro documento su un web server *convenzionale*, dobbiamo cominciare seguendo la ricetta di come scegliere un servizio di hosting web[15].
Nella maggior parte dei casi, la pubblicazione avverrà tramite un browser web. Seguiamo quindi la ricetta "visitare siti web" tra i casi d'impiego precedenti[16].
Grazie agli onion service[17] di Tor, è anche possibile ospitare in proprio il nostro documento: gli onion service permettono di mettere a disposizione un web server o un altro tipo di server senza dover rivelare il proprio indirizzo IP. Non utilizzano un indirizzo pubblico e quindi possono funzionare facilmente dietro un firewall[18] o un'altra macchina che si occupi di fare la traduzione degli indirizzi di rete (NAT)[19].
Se preferiamo ospitare il nostro documento su un onion service, bisogna seguire la ricetta "Usare OnionShare"[20].

### 9.3.4 Terza strategia d'attacco: guardare sul computer utilizzato

Questa strategia è simile a quella descritta nella sezione analoga del caso d'impiego precedente[21]. Vi invitiamo quindi ad andare a leggervelo (o rileggervelo).

---

14 Cap. 2.1.3
15 Cap. 15
16 Cap. 8.5
17 Cap. 7.1.3
18 Cap. 1.2.6
19 Cap. 1.3.4
20 Cap. 22
21 Cap. 8.3.2

### 9.3.5 Quarta strategia d'attacco: attaccare Tor

Nella disperazione, l'avversario può anche decidere di provare ad attaccare Tor. Rimandiamo alla sezione analoga del caso d'impiego precedente[22].

## 9.4 Contatto pubblico

Quando pubblichiamo un documento, potremmo voler essere contattati dalle persone che lo hanno letto. Questa necessità apre nuove possibilità di attacco a un avversario alla ricerca di falle da sfruttare.
Se abbiamo preso tutte le precauzioni per essere il più anonimi possibile durante la pubblicazione del documento, ma poi il nostro indirizzo per essere contattati è: nome.cognome@ esempio.org, siamo punto e a capo. Per evitare un errore del genere, sarà bene avere uno pseudonimo[23] da usare unicamente per questo documento o una serie di documenti a seconda dell'identità contestuale[24] che vogliamo adottare.
L'avversario cercherà allora di scoprire chi si nasconde dietro a questo pseudonimo. Per provare a mascherare "chi utilizza questo indirizzo email", può aiutarci il caso d'impiego "Scambiarsi email celando la propria identità"[25].
Infine, potremmo voler nascondere il contenuto[26] delle email scambiate, ma questo potrebbe diventare molto complesso: nella misura in cui sentiamo la necessità di un indirizzo di contatto pubblico, l'*accessibilità* può entrare in conflitto con la discrezione.

---

22 Cap. 8.3.3
23 Cap. 5.1.1
24 Cap. 5.2
25 Cap. 10.7
26 Cap. 10.8

Se mettiamo in atto tutto un insieme di precauzioni per aumentare l'anonimato del nostro contatto, difficilmente riusciremo ad avere anche il resto. Le persone che vogliono contattarci potrebbero mettersi in pericolo dialogando con noi, senza pensare al proprio anonimato. Ricordare ed esplicitare le condizioni di confidenzialità e di anonimato diventa quindi indispensabile. Inoltre non sappiamo mai chi ci sta contattando veramente, bisogna fare attenzione a cosa si racconta se non vogliamo comprometterci.

# 10 | Caso d'impiego: scambiarsi dei messaggi

## 10.1 Contesto

Adesso abbiamo bisogno di scambiare dei messaggi con altre persone. Magari perché vogliamo augurare buon compleanno alla mamma, magari perché stiamo lavorando insieme a un documento sensibile[1]. Non ci interessa la sincronicità dello scambio: al contrario di quando parliamo di una conversazione telefonica o di un dialogo in chat, in questo caso specifico ci riferiamo a una comunicazione asincrona.
Più avanti parleremo anche delle conversazioni sincrone[2]. Ma per il momento concentriamoci sulla posta elettronica: l'e-mail.

## 10.2 Valutare i rischi

### 10.2.1 Cosa vogliamo proteggere?

Quando viene inviata una email, c'è la possibilità che diverse informazioni possano trapelare fino al nostro avversario. Quali?
Quando ci poniamo questa domanda prima di tutto ci viene in mente il contenuto del messaggio. Anche se non necessariamente tutti i nostri messaggi devono essere top-secret, alcuni meritano una discrezione maggiore di altri: sia che si voglia evitare che vengano diffusi i dettagli delle nostre relazioni intime, sia che pensiamo che il contenuto di un messaggio possa farci arrivare guai come un licenziamento o un bel soggiorno in carcere. Ma, in generale, magari non siamo esattamente

1 Tomo I, cap. 9
2 Cap. 11

entusiasti all'idea che il postino possa leggersi tutte le lettere che abbiamo ricevuto negli anni passati, in attesa di quelle che arriveranno domani. Se effettuiamo la nostra corrispondenza email senza prendere precauzioni particolari, chi sta nel mezzo potrebbe leggere le nostre comunicazioni in modo completamente trasparente, come fossero cartoline.
Ma oltre al contenuto della cartolina, potrebbe essere interessante mascherare anche le informazioni contestuali come la data della comunicazione, le identità dei protagonisti, dove si trovavano in quel momento, ecc. Questi dettagli possono essere rivelati per esempio nelle intestazioni HTTP[3], negli header delle email[4], o nel corpo stesso del messaggio[5].
Già il fatto che una certa persona stia scrivendo a un'altra può costituire di per sé un'informazione sensibile. Succede spesso che le relazioni tra le persone vengano analizzate attraverso certe forme di sorveglianza, per derivarne ad esempio una rete di oppositori politici[6]. Queste tracce generalmente si trovano nelle intestazioni delle email[7] e nei log di connessione[8].

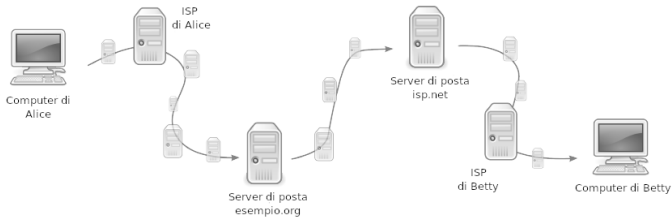
### 10.2.2 Da chi vogliamo proteggerci?

Potremmo voler offuscare tutte o una parte di queste informazioni agli occhi delle diverse macchine che potrebbero accedervi e alle persone che hanno accesso a queste macchine.
Tra queste, in primo luogo, ci sono i server coinvolti. Come minimo, per ciascun messaggio inviato da Alice (`alice@esempio.org`) a Betty (`betty@provider.net`) avremo:

3 Cap. 2.4.1
4 Cap. 2.4.2
5 Cap. 2.5
6 Jean-Marc Manach, 2011, *Réfugiés sur écoute* [rasufi.vado.li].
7 Cap. 2.4.2
8 Cap. 2.3

- il server incaricato da Alice di inviare il messaggio: generalmente questo server sarà quello di `esempio.org`;
- il server incaricato di ricevere il messaggio e conservarlo nella casella di posta di Betty: `provider.net`.

Ma c'è dell'altro. Lungo il percorso sono situati molti altri computer[9] (i router), e hanno accesso[10] alle informazioni che trasportano:

- tra il computer di Alice e il provider;
- tra il provider di Alice e il suo server di posta `esempio.org`;
- tra esempio.org e il server mail di Betty, `provider.net`;
- quando Betty consulterà la propria casella di posta, il messaggio viaggerà tra il server mail `provider.net` ed il proprio provider;
- infine, tra il provider di Betty e il suo computer.

*Schema di utilizzo di un circuito Tor*

Gli amministratori di queste macchine sono i primi ad avere accesso a questo tipo di informazioni, ma non sono necessariamente i soli. Questi dati possono essere rintracciati da pirati[11]

9 Cap. 1.4.1
10 Cap. 2.3
11 Cap. 3.4.2

più o meno governativi, muniti o no di mandato legale[12].
Infine, ciascuna consultazione di una casella di posta, ciascun invio di messaggi, rischia di lasciare tracce[13] sul computer utilizzato. Sarà bene nasconderle ai curiosi che potrebbero essere in grado di sbirciare nei nostri hard-disk.

## 10.3 Due problematiche

Potremmo avere come obiettivo quello di proteggere al tempo stesso sia la nostra identità – così come quella dei nostri destinatari – sia il contenuto della comunicazione. Si tratta quindi delle informazioni che sono contenute in entrambe le parti della nostra casella postale: nel testo e nelle intestazioni. Queste informazioni sono visibili per tutto il tragitto compiuto dai nostri messaggi e possono essere bersaglio di attacchi. La policy di sicurezza che andremo a definire dipenderà soprattutto dal modo in cui consultiamo le email. I diversi modi possono prevedere differenti protocolli[14] che non comportano le stesse conseguenze in termini di tracce lasciate.

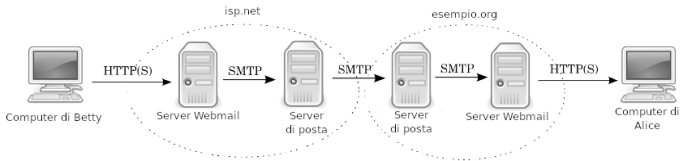
## 10.4 Webmail o client mail?

Esistono due modi di consultare l'email: si può usare una webmail oppure un client mail. Questa scelta dipende da diversi fattori, tenendo conto che una sola casella email può anche utilizzarli entrambi e che la scelta di uno o dell'altro non è irreversibile.

---

12 Cap. 3.2.4
13 Tomo I, cap. 2
14 Cap. 1.2.3

## 10.5 Webmail

Una webmail è un sito web che permette di consultare le proprie email attraverso un browser web. Il suo utilizzo si è diffuso a macchia d'olio dall'inizio degli anni 2000, a tal punto che abbiamo quasi dimenticato gli altri modi per consultarle. Hotmail e Gmail sono degli esempi molto famosi di servizi che incentivano il suo utilizzo (nonostante siano usabili anche tramite client). Ancora una volta, abbiamo a che fare con una tendenza del Web 2.0[15]: non occorre più avere il proprio sistema operativo per accedere alla propria casella di posta (che sia sul computer o su una penna USB contenente un sistema live). Basta soltanto avere un accesso a internet.

*Alice e Betty utilizzano una webmail*

La webmail in fin dei conti è un'interfaccia web che ci permette di agire su dei server mail. Schematizziamo uno scambio di email tra Alice e Betty, che utilizzano entrambe la webmail:

- il percorso di rete (il routing) tra il computer di Betty e la sua casella di posta ospitata da `provider.net` sarà percorso attraverso un protocollo web (HTTP ou HTTPS);
- seguirà un piccolo tragitto all'interno di `provider.net` che assicurerà il transito dalla webmail alla email;
- poi un viaggio tramite il protocollo email (SMTP) tra

15 Cap. 4

`provider.net` e `esempio.org`;
- di nuovo un piccolo pezzo all'interno questa volta di `esempio.org`, tra il protocollo email e il web;
- poi dal web (HTTP o HTTPS) fino al computer di Alice.

### 10.5.1 Vantaggi

Tra i vantaggi della webmail, così come per ciascuna applicazione web, possiamo annoverare l'assenza di installazione, di aggiornamenti e di configurazione, cose che invece occorre fare se scegliamo un client mail. C'è inoltre il vantaggio principe del Web 2.0: la possibilità di accedere alla propria posta da qualsiasi computer connesso a internet, da ovunque e in qualsiasi momento.

### 10.5.2 Svantaggi

Per contro, c'è il fatto che in caso di assenza di connessione, tutta la nostra corrispondenza ci è inaccessibile (a meno che non ce la siamo salvata[16] tutta o in parte su un supporto portatile: penna USB, hard-disk, ecc.).
Il fatto che sia possibile utilizzare un *qualsiasi* browser web per accedere alla nostra casella di posta, può facilmente indurci a utilizzarne uno a caso, magari attraverso un computer di cui faremmo bene a non fidarci.
Inoltre, a seconda di quanto ci fidiamo del servizio che ospita la nostra posta, conviene porsi la questione della centralizzazione dei nostri dati. L'uso massivo della webmail ha portato a concentrare migliaia di caselle di posta, con tutto il loro contenuto, nelle mani dei grandi fornitori di servizi di posta,

---

16 Cap. 19

affidandogli in questo modo una montagna di dati personali. Questi servizi potrebbero utilizzarli a scopi commerciali, consegnarli a diverse autorità, o anche soltanto perderli. In più se riteniamo la nostra corrispondenza sensibile per un motivo o per un altro, magari preferiremmo non affidarla a nessuno – ricordiamoci che ci sono persone dietro alle macchine – che non abbia particolarmente voglia di farsi carico di questa responsabilità. Questo probabilmente è stato il caso dell'agosto 2013, quando la società Lavabit[17] che ospitava la casella di posta di Edward Snowden ha deciso di chiudere battenti. La chiusura è stata decisa in seguito alle pressioni da parte di agenzie governative come l'NSA e l'FBI.
Infine, l'utilizzo della webmail può essere riempito di pubblicità che appariranno sul nostro browser web mentre stiamo leggendo la posta. Pubblicità che potrebbero anche essere scelte in base al contenuto delle nostre email[18].

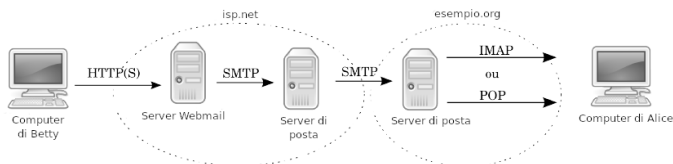
## 10.6 Client mail

Un client mail è un programma che serve a gestire le proprie email: a riceverle, leggerle, inviarle ecc. Alcuni client di posta diffusi sono per esempio Outlook di Microsoft oppure Thunderbird di Mozilla. Ne esistono molti altri che, malgrado le differenze, possiedono un'interfaccia grossomodo simile, somigliante a quella della webmail.
Contrariamente alla webmail, in cui andiamo a consultare le nostre email sul server del gestore di posta utilizzando un browser, qui la lettura della posta viene effettuata grazie a un programma installato sul computer. Le email vengono salvate in un dispositivo di archiviazione locale (l'hard-disk del computer, una penna USB, ecc.).

17 Wikipedia, *Lavabit*.
18 Cap. 3.1.1

Per riprendere il nostro piccolo schema di prima, sostituiamo i protocolli web con dei protocolli di posta. Per ricevere la posta esistono due diversi protocolli, IMAP (Internet Message Access Protocol) e POP (Post Office Protocol).
Il primo, IMAP, permette di lasciare le email sul server di posta del nostro gestore. Ogni volta che ci connettiamo con la nostra casella di posta, avviene una sincronizzazione in modo da conservare la stessa situazione (numero di email, bozze, cartelle, ecc.) sia sul server che sul nostro programma di posta. Questo senza doversi scaricare tutto il contenuto presente sul server. Per esempio sul nostro client potrebbero essere scaricate solo le intestazioni delle email.
Il secondo protocollo, *POP*, scaricherà i vari dati contenuti nella casella di posta direttamente sul nostro client, senza necessariamente lasciarne una copia sul server remoto.

### 10.6.1 Vantaggi

I pro e i contro dipendono in larga misura dal protocollo utilizzato per ricevere. Betty utilizza una webmail, Alice un client di posta la posta, ma i primi che affronteremo riguardano entrambi.

*Betty utilizza una webmail, Alice un client di posta*

Prima di tutto, con un client di posta possiamo accedere alla nostra casella di posta trovandola come la si era lasciata, anche in assenza di connessione a internet. Possiamo insomma leggere, scrivere e cancellare email anche se siamo offline, senza ovviamente poter inviare e ricevere. Inoltre l'utilizzo di un client mail ci risparmia di doverci sorbire la miriade di pubblicità di cui il web è infarcito.
Utilizzando il protocollo POP, beneficiamo di altri vantaggi come la decentralizzazione della posta. Invece di lasciare tutta la nostra corrispondenza su dei server remoti, le email vengono importate sul computer. Questo ci evita di dover lasciare a tempo indefinito tutte le nostre email ai maggiori fornitori di servizi di posta, e anche di non consumare troppo spazio nel caso fossimo invece ospitati da piccoli servizi. Il fatto che le email finiscano sul sistema del destinatario ci consente un controllo maggiore su come vengono gestite: per esempio nel caso in cui servisse eliminare definitivamente e sul serio delle email pericolose. Infine, in questo modo stiamo lasciando meno dati alle aziende che non rispettano la confidenzialità delle corrispondenze.
Nonostante ciò, attenzione: le nostre email transitano lo stesso attraverso il servizio di posta, che potrà decidere di leggerle e eventualmente copiarle prima che noi le importiamo.

### 10.6.2 Svantaggi

Per utilizzare un client mail occorre configurare un programma di posta in modo da dirgli quale casella controllare, a quale server si deve connettere e quale protocollo deve usare.
Quindi è un po' più complicato consultare la posta da un computer che non è il nostro (se siamo da degli amici oppure al lavoro, per esempio), a meno di utilizzare il client di posta di un sistema live persistente (come quello di Tails), installato

su una penna USB.
Inoltre, nel caso in cui stiamo utilizzando il protocollo POP, il dispositivo di archiviazione sul quale si trovano le nostre email sarà l'unico in cui si trova la nostra posta. Se questo dispositivo si rompe (sia che fosse un hard-disk oppure la penna USB sul quale avevamo installato la live persistente di Tails), possiamo dire addio a tutti i nostri preziosi messaggi... a meno che non avessimo pensato prima a fare un backup[19].

## 10.7 Scambiarsi email nascondendo la propria identità

L'obiettivo in questo caso è quello di nascondere a un avversario che siamo uno dei due interlocutori di uno scambio di email. Potrebbe trattarsi di una corrispondenza con un dissidente politico ricercato, ma anche con un'amica che avevamo perso di vista.

### 10.7.1 Definire una policy di sicurezza

Il nostro scopo principale è quello di nascondere i nomi delle persone che si stanno scambiando le email, o perlomeno di rendere la loro identificazione quanto più difficile possibile.

#### Prima strategia di attacco: chiedere ai fornitori

Il nostro fornitore di servizi di posta è un nodo della rete attraverso il quale, per forza di cose, transita la nostra corrispondenza. Un avversario avrebbe quindi ottime ragioni per darci un'occhiata, tanto più che questo lavoro potrebbe risultargli estremamente facile.

19 Tomo I, cap. 19

Allo stesso modo, agli intermediari tra Betty e Alice, i loro rispettivi ISP, basterebbe guardare nel posto giusto per leggere le intestazioni delle email[20], che possono rivelare moltissime informazioni tra le quali, presso alcuni servizi, gli stessi indirizzi IP corrispondenti. Questo tipo di attacco è più che probabile nel caso in cui il contenuto delle email o i protagonisti della corrispondenza attirino l'attenzione di un'autorità che ha abbastanza potere. Ci sembra comunque importante suggerire come prima cosa che evitare di utilizzare una casella del tipo `nome.cognome@esempio.org` è già un buon punto di partenza. Dobbiamo quindi pensare a uno pseudonimo, in modo da costruire un'identità contestuale[21].

Detto ciò, se "Kiwi Poilu" scrive regolarmente a Caroline Carot, Sofiane Carot e Francine Carot, un avversario *potrebbe* pensare che Kiwi Poilu sia qualcuno che appartiene alla famiglia Carot, o che comunque faccia parte della cerchia degli amici intimi: le identità dei destinatari sono anch'esse rivelatrici.

Inoltre se stiamo utilizzando uno pseudonimo, ma un avversario osserva che le email che sta sorvegliando partono da un determinato appartamento, può risalire a noi. Funziona come per la navigazione sul web: l'utilizzo del routing Tor[22] o di un sistema live amnesico evita questo tipo di problemi confondendo le tracce che porterebbero al nostro computer.

Infine, il contenuto della corrispondenza può essere sufficiente per permettere di indovinare i nomi degli autori. Nascondere un'identità necessita insomma di fare attenzione non soltanto alle intestazioni, ma anche al contenuto della email.

Per proteggere il contenuto delle email dagli sguardi curiosi, sia in se stesso, sia perché potrebbe contenere informazioni sugli autori delle email, dobbiamo utilizzare la posta cifrata[23].

---

20 Cap. 2.4.2

21 Cap. 5

22 Tomo I, cap. 14

23 Cap. 10.8

**Seconda strategia di attacco: guardare sul computer utilizzato**
Se per proteggere la nostra identità viene usato uno pseudonimo e la rete Tor, un potenziale attaccante potrebbe provare ad accedere alle tracce lasciate sul computer[24], in modo da provare che la persona che sospetta sia proprio quella che controlla la casella di posta in questione.
Per premunirsi da questo attacco è necessario cifrare il proprio hard-disk[25] oppure, meglio ancora, evitare in partenza di lasciare queste tracce, utilizzando un sistema live amnesico[26].
Questo è ancora più importante se stiamo utilizzando un client mail, perché ad essere lasciate sul computer non sono soltanto le tracce, ma anche le email vere e proprie.

**Terza strategia di attacco: attaccare Tor**
Un attaccante che è in grado di sorvegliare vari punti della rete, per esempio la connessione utilizzata *e* il fornitore di servizi di posta, potrebbe essere in grado di sbaragliare l'anonimato fornito dalla rete Tor.
Ricordiamo ancora una volta che ci sono numerosi altri temibili attacchi possibili contro la rete Tor, e che è d'obbligo sapere bene da cosa ci protegge[27] e da cosa no[28].

### 10.7.2 Scegliere tra gli strumenti disponibili

Esistono diversi strumenti disponibili per comunicare via email, la scelta va quindi fatta in funzione dei diversi criteri che abbiamo evocato precedentemente. Per esempio possiamo

24 Tomo I, cap. 2
25 Tomo I, cap. 15
26 Tomo I, cap. 14
27 Cap. 7.1.2
28 Cap. 7.3

preferire di non lasciare le nostre email sul server del nostro servizio di posta, leggerle e rispondere offline, oppure al contrario di non scaricarne una copia in locale, ma invece accedervi ogni volta via web.

### 10.7.3 Webmail

Essendo la webmail uno strumento specifico del web, dovremo fare riferimento alle questioni relative al Tor Browser o a Tails – ai loro pro e ai loro contro, a come si utilizzano... – e al caso d'impiego che spiega la navigazione web[29]. I certificati o le Certification Authority usati per cifrare la connessione verso il server di posta devono essere autentici, perché un attaccante in grado di ingannare l'utente sarebbe capace di recuperare tutti gli scambi in chiaro con il server di posta, tra cui login e password della casella email. Dovremo quindi farci carico di verificarli[30].
Inoltre, se si utilizza la webmail all'interno di Tails su un computer su cui nutriamo sospetti, soprattutto che possano avvenire attacchi di tipo keylogger[31], al momento di inserire la password della nostra casella di posta dovremo usare una tastiera virtuale[32].

### 10.7.4 Client mail

Se preferiamo utilizzare un client mail invece della webmail, possiamo, a scelta:

29 Cap. 8
30 Cap. 16
31 Tomo I, cap. 3.4
32 Cap. 17

- utilizzare Tails[33], nel quale è incluso il client Thunderbird[34]. In questo modo le tracce lasciate in locale saranno eliminate con lo spegnimento del sistema;
- utilizzare Tails e Thunderbird con la persistenza[35]. Il contenuto della nostra casella di posta sarà archiviato su una penna USB che conterrà delle tracce, ma cifrate;
- installare un client mail sul nostro sistema cifrato. Installare il pacchetto Thunderbird seguendo la ricetta “installare un programma”[36];
- seguire la ricetta “utilizzare Thunderbird”[37]. In questo modo però verranno lasciate tracce sull’hard-disk del computer.

Ma anche qui, come nel caso della webmail, bisognerà farsi carico di verificare i certificati o le Certification Authority[38] che cifrano la connessione verso il servizio di posta.

## 10.8 Scambiarsi delle email confidenziali (e autenticate)

In questo caso ciò che vogliamo è nascondere il contenuto delle nostre email, in modo da evitare che altre persone oltre al destinatario possano leggerlo, sia nel caso in cui il contenuto dei nostri messaggi sia *sensibile*, sia che riveli dettagli sulla persona che li ha scritti.
Per definire la nostra policy di sicurezza, dobbiamo considerare l’utilizzo della crittografia secondo diverse modalità.

33 Tomo I, cap. 14
34 Cap. 18
35 Tomo I, cap. 14.4
36 Tomo I, cap. 16
37 Cap. 18
38 Cap. 16

### 10.8.1 Prima strategia di attacco: chiedere ai fornitori

Se non mettiamo in campo nessuna misura di protezione particolare, i fornitori di servizi di posta potranno leggere il contenuto delle email che riceviamo. È proprio sui loro server che vengono instradate e archiviate le nostre email.

*Connessione non cifrata ai server di posta*

I nostri messaggi potrebbero essere conservati per anni, finché non li scarichiamo o eliminiamo, o per un tempo ancora maggiore se uno dei server se li fosse copiati, magari per un backup. Da qui l'importanza di chiudere le caselle di posta una volta che la loro ragion d'essere è finita. Anche per non occupare inutilmente lo spazio hard-disk del fornitore di servizi di posta.

*Nel frattempo, e a condizione che ci piaccia smanettare, è possibile mettere su un proprio server mail su un Onion Service di Tor*[39]*.*

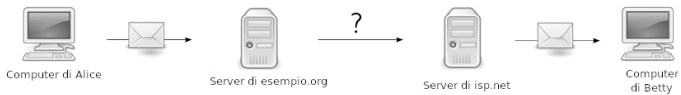
Tra usare un protocollo o l'altro, la webmail o il client, non c'è una grande differenza. L'uso del protocollo POP con un client mail ben configurato (quindi che scarica completamente le email e che le cancella dal server remoto), a patto di controllare con regolarità la casella, al massimo eviterà di lasciare la nostra posta a fare la muffa sui server dei nostri fornitori.

39 Cap. 7.1.3

Leggere i nostri messaggi, violando la segretezza della nostra corrispondenza – come leggere una lettera indirizzata a noi – non richiede alcuno sforzo tecnico, neanche quello di aprire la busta. Si tratta di un'azione talmente facile da essere addirittura automatizzata in Gmail: questi fa leggere il contenuto delle email da "robot" per individuare lo spam, nonché per profilare meglio i propri utenti al fine di, tra le altre cose, "offrire" la pubblicità più adatta a loro.

*Questi "robot" non sono né automi né androidi, ma dei piccoli programmi che scorrono "automaticamente" un contenuto per trovare qualcosa: per esempio, i "robot" di Google scorrono le pagine web per indicizzare le parole chiave pertinenti che potrebbero essere cercate nel motore di ricerca. Questi stessi robot vengono utilizzati anche dalle guardie per farsi segnalare ogni volta che qualcuno utilizza delle parole che rientrano all'interno del loro supposto "dizionario dei terroristi".*

Per quanto riguarda gli intrusi che si mettono in mezzo tra i protagonisti dello scambio email e i rispettivi fornitori di servizi di posta, possiamo trovarci di fronte a due situazioni. La prima, ormai piuttosto rara, è quella in cui la connessione tra un protagonista e il suo server mail non sia cifrata. In questo caso, i diversi intrusi si vedranno passare tra le mani delle cartoline postali. Saranno insomma in una situazione simile a quella dei fornitori di servizi di posta, con la differenza che le cartoline postali sarebbero solo fatte passare... salvo il caso in cui gli venisse l'idea di gettare uno sguardo più approfondito alla posta che stanno trasportando, magari per fare delle statistiche al fine di migliorare i propri servizi, o magari perché qualcuno gliel'ha gentilmente chiesto.
La seconda situazione è quella in cui la connessione tra un protagonista e il suo server di posta è cifrata con il protocollo TLS. A prescindere dal protocollo utilizzato, gli intrusi po-

sizionati in mezzo tra un protagonista e il proprio server di posta, questa volta si vedranno passare tra le mani delle cartoline postali chiuse in delle buste. Buste più o meno difficili da aprire: in effetti, anche se la connessione tra Alice e il proprio server di posta è davvero cifrata[40], Alice non sceglie però in quale modo[41]. Inoltre il fornitore di servizi di posta non subisce la stessa cifratura e avrà accesso alle email nella loro interezza. Per usufruire di una connessione cifrata in modo efficace, non dobbiamo fidarci ciecamente di una Certification Authority, né accettare un certificato senza averlo prima verificato[42].
Infine, niente ci garantisce che la connessione tra il server di posta di Alice e quello di Betty venga cifrata ogni volta, e potrebbe succedere che il tragitto della email si svolga a volte in forma di cartolina postale e altre volte in quella di lettera imbustata.

*Connessione non cifrata ai server di posta*

Per assicurarsi che il contenuto dei nostri messaggi non sia letto da nessun intruso, fornitore compreso, dobbiamo cifrare il messaggio direttamente sul nostro computer, prima di inviarlo. Per farlo, dobbiamo utilizzare lo standard di crittografia asmimmetrica OpenPGP. Potremmo anche utilizzare la crittografia simmetrica, ma i suoi limiti[43] ci spingono a sconsi-

40 Cap. 6
41 Cap. 6.4.2
42 Cap. 16
43 Cap. 6

gliarla fortemente.
Quando usiamo la crittografia asimmetrica, soltanto la persona destinataria, per la quale avremo effettuato la cifratura, sarà effettivamente in grado di decifrare il messaggio. Non dimentichiamo però che la crittografia asimmetrica possiede anche dei limiti[44] che potrebbero permettere a un avversario di riuscire a decifrare un contenuto cifrato.
In pratica, se non l'abbiamo già fatto, si inizia importando[45] la chiave pubblica del nostro destinatario. Poi se ne verifica l'autenticità[46]. In più, se si ha intenzione di stabilire una corrispondenza e quindi non solo spedire, ma anche ricevere delle risposte, dobbiamo disporre anche di una nostra coppia di chiavi: una sarà usata dai nostri corrispondenti per inviarci delle email cifrate, l'altra ci permetterà di decifrarle. Se non abbiamo ancora una coppia di chiavi di cifratura, seguiamo la ricetta per crearle[47] e gestirle correttamente.
Dopo aver scritto il messaggio, seguiamo la procedura necessaria per cifrarlo[48]. A questo punto non resta che inviarlo!
Però attenzione, questo metodo permette di cifrare il contenuto e soltanto questo. Le intestazioni[49] della email rimarranno intatte.

### 10.8.2 Seconda strategia d'attacco: guardare sul computer utilizzato

Supponiamo che un attaccante non abbia accesso ai dati del nostro fornitore di servizi di posta, e che non possa intercet-

44 Cap. 6.6
45 Cap. 19.1
46 Cap. 19.2
47 Cap. 19.4
48 Cap. 19.6
49 Cap. 2.4.2

tare la rete, ma che sia invece in grado di curiosare in casa nostra: quali tracce troverebbe sul nostro computer?
Se questo avversario mettesse le mani sul nostro computer o su quello dell'altra persona coinvolta nella comunicazione, magari prendendoselo oppure attraverso l'installazione di un software malevolo[50], potrebbe avere accesso a tutte le email archiviate e alle tracce lasciate. Tracce dovute al funzionamento del computer o lasciate dai protagonisti.
Per proteggersi da questo attacco bisogna imparare a cifrare il nostro hard-disk[51] in modo da rendere più complicato all'avversario l'accesso ai dati in esso contenuti. Questo però non ci proteggerà da un software malevolo in grado di esfiltrare i dati, per questo è importante installare soltanto programmi fidati. Altrimenti possiamo utilizzare un sistema live amnesico.
Teniamo conto che se le email salvate fanno parte di una corrispondenza che è stata cifrata attraverso la crittografia asimmetrica, anche avendo accesso al computer l'avversario non potrebbe comunque leggerle, a meno di non avere accesso alla chiave segreta e di scoprire la password che permette di usarla.

### 10.8.3 Terza strategia d'attacco: attaccare la cifratura del dispositivo

Se consultiamo le nostre email su una Debian cifrata, le tracce sull'hard-disk del computer verranno cifrate, sia che si utilizzi la webmail che un client mail. Di per se stesse quindi non diranno niente a un avversario. Alcuni avversari però potrebbero avere i mezzi per attaccare questa cifratura[52]. Inoltre, se la persona con cui stiamo conversando non utilizza le stesse nostre precauzioni, il livello globale di protezione del contenuto si ab-

50 Tomo I, cap. 3
51 Tomo I, cap. 15
52 Tomo I, cap. 5.1.4

basserà a quello della più fragile fra le due protezioni. In effetti, il prendere grandi precauzioni e poi scambiare email con una persona che magari non utilizza una Debian cifrata, o che la tiene sempre accesa[53], può essere più pericoloso ancora perché ci dà una sensazione di falsa sicurezza. Tanto più se è facile localizzare o dare un nome ai protagonisti della corrispondenza.
Se si utilizza un programma di posta all'interno di un sistema live amnesico, dopo lo spegnimento non lasceremo alcuna traccia sul computer, ma ne resteranno sulla partizione persistente, se l'abbiamo configurata. Queste ultime tracce saranno cifrate, il che ci riporta al caso della Debian cifrata.
Per non lasciare alcuna traccia, cifrata o no, sul computer, possiamo utilizzare il sistema live Tails senza la persistenza e usufruire in questo modo della sua modalità amnesica.

### 10.8.4 Quarta strategia d'attacco: attaccare la crittografia dei messaggi

Un avversario che riuscisse, in un modo o in un altro, a mettere le mani sulle email cifrate, potrebbe provare a forzarne la cifratura sfruttando i vari limiti della crittografia[54].

53 Un computer con l'hard-disk cifrato finché è acceso contiene molte informazioni in chiaro nella sua RAM [tomo I, cap. 1.2.3].
54 Tomo I, cap. 5.1.4

# 11 | Caso d'impiego: conversare

## 11.1 Contesto

Nel precedente caso d'impiego, scambiavamo messaggi in modo asincrono[1], come nel caso di uno scambio epistolare. Però potremmo invece volere una comunicazione sincrona, come quella di una conversazione telefonica, per una riunione di lavoro su un documento sensibile[2] o per chiacchierare con un'amica. Il modo più semplice potrebbe essere quello di uscire di casa e incontrarsi, oppure di chiamarsi al telefono, ma non sempre è possibile o consigliabile e potrebbe anche creare problemi. A volte quindi la messaggistica istantanea è una buona alternativa.
Molte persone conoscono e utilizzano regolarmente Skype (che rimpiazza MSN o Windows Live Messenger forniti da Microsoft) o la messaggistica interna a Facebook, tanto per citare alcuni esempi tra i più noti. È pratico, sì, ma esistono anche strumenti altrettanto pratici che ti permettono di non rinunciare all'essere discreti!

## 11.2 Valutare i rischi

### 11.2.1 Che cosa vogliamo proteggere?

Le risposte a questa domanda sono le stesse del caso dello scambio di email[3]. Potremmo voler proteggere il contenuto della corrispondenza, la localizzazione dei protagonisti, la loro identità, i loro legami, ecc.

1 Cap. 10
2 Tomo I, cap. 9
3 Cap. 10

## 11.3 Definire una policy di sicurezza

Poniamoci adesso le domande elencate nel nostro metodo[4], adottando il punto di vista del nostro avversario.

### 11.3.1 Prima strategia d'attacco: tutte le informazioni a disposizione dei curiosi

La messaggistica interna di Facebook, Skype, ecc. permettono a molte persone di acquisire informazioni che non li riguardano: Facebook o Microsoft vedono passare per intero le nostre conversazioni sulle loro macchine e possono salvarle per accedervi poi in seguito. Le guardie poi non hanno che da chiedere per poter beneficiare di queste informazioni e una falla di sicurezza sui server può dare accesso anche a numerosi altri curiosi. Senza dimenticare inoltre che Facebook cambia regolarmente le proprie policy sulla sicurezza senza avvisare prima, e può decidere da un giorno all'altro di rendere pubblico ciò che oggi è "privato".
Inoltre Skype registra le conversazioni sul computer che stiamo utilizzando e quindi qualunque vicino, ladro o amante geloso potrebbero accedere a questo storico.
Ma Microsoft e Facebook non hanno inventato la messaggistica istantanea, e ci sono svariate alternative. Esistono molti programmi che possiamo installare sul nostro computer e che ci permettono di comunicare attraverso diversi protocolli: Skype, IRC, XMPP, ecc.
Utilizzare un programma di cui ci fidiamo ci permetterà di disattivare il salvataggio delle conversazioni e quindi limitare le tracce lasciate sul nostro computer.
Esistono anche dei fornitori di servizi che offrono degli indiriz-

4 Tomo I, cap. 7

zi di messaggistica istantanea e che non sono in una posizione tale da permettergli di rastrellare tanti dati quanto Google, Microsoft o Facebook.
Per seguire questa soluzione su un sistema Debian (cifrato) installato precedentemente[5], ci possiamo rifare alla ricetta "installare un programma"[6] e possiamo installare Pidgin. Se stiamo utilizzando Tails, questo programma lo troviamo già installato.

### 11.3.2 Seconda strategia d'attacco: chiedere ai fornitori

Se utilizziamo un client di messaggistica istantanea e diversi server, evitiamo di concentrare tutti i collegamenti e le conversazioni nelle stesse mani. Nonostante ciò, il contenuto delle conversazioni e tutte le parti che comunicano resteranno accessibili nei computer attraverso i quali transitano.
Se anche è possibile configurare il nostro client in modo da cifrare la connessione fino al server di messaggistica, le conversazioni resteranno accessibili al server. Inoltre non possiamo essere certi che anche il collegamento tra il server e quello della persona con cui stiamo conversando sia cifrato.
Un avversario che ne sia in grado[7] potrebbe quindi rivolgersi agli amministratori del server, oppure alle aziende che forniscono la connessione, per ottenere delle informazioni sulle conversazioni. Si potrà anche tentare di fare intrusione nelle sue macchine[8].
La confidenzialità delle conversazioni resta quindi fortemente legata alla fiducia che riponiamo nei servizi di messaggistica

5 Tomo I, cap. 15
6 Tomo I, cap. 16
7 Cap. 3.2.4
8 Cap. 3.4.2

che stiamo utilizzando, o nelle infrastrutture di rete, in particolare nel nostro provider.
Per complicare di molto la vita a un avversario che vuole leggere il contenuto delle nostre conversazioni, possiamo utilizzare la crittografia end-to-end[9] e ottenere in questo modo riservatezza. Sfortunatamente, attualmente non esistono implementazioni della crittografia end-to-end che permettano le conversazioni di questo tipo in gruppo. Questa soluzione è limitata alle discussioni a due.
Per seguire questo metodo su un sistema Debian (cifrato) installato in precedenza[10], seguiamo la ricetta "Installare un software"[11] e installiamo il pacchetto `pidgin-otr`. Da quel momento possiamo utilizzare la messaggistica istantanea cifrata con OTR[12].

### 11.3.3 Terza strategia d'attacco: i collegamenti restano visibili

Se adoperiamo la crittografia end-to-end durante una conversazione di messaggistica istantanea, un avversario non riuscirà più ad accedere al contenuto della conversazione, a meno di non rompere l'algoritmo di cifratura usato[13], accedere al nostro computer[14] o hackerarlo.
Ciò nonostante, un avversario che riuscisse ad avere accesso alla connessione o al server di messaggistica potrebbe continuare a vedere con chi stiamo parlando. Per nascondere questi collegamenti, dobbiamo usare delle identità contestuali[15] e

---

9 Cap. 6
10 Tomo I, cap. 15
11 Tomo I, cap. 16
12 Cap. 20
13 Cap. 6.6
14 Cap. 3.4.4
15 Cap. 5

connetterci in modo anonimo, per esempio utilizzando Tor[16]. In questo modo avremo *riservatezza*, grazie alla crittografia, ma anche *pseudonimato*.
Quando usiamo un sistema live amnesico come Tails, ci stiamo occupando in un colpo solo anche della questione delle tracce che potrebbero essere lasciate sul computer. Questo a meno di non stare usando la persistenza, in tal caso alcune tracce rimarrebbero nella partizione persistente all'interno della penna USB di Tails.
Per seguire questa ricetta dobbiamo procurarci, se non ce l'abbiamo già, una penna USB o un DVD con Tails[17].
Successivamente, dopo aver avviato dal dispositivo con sopra Tails[18], dovremo stabilire un'identità contestuale da utilizzare e configurare la persistenza di Tails[19] per questa identità, attivando l'opzione "Pidgin".
Infine non ci resta che seguire la ricetta per utilizzare la messaggistica istantanea con OTR[20].
In questo caso stiamo combinando due criteri: riservatezza e anonimato. Nella strategia d'attacco precedente abbiamo visto come ottenere la *riservatezza* attraverso la crittografia end-to-end. Adesso stiamo sperimentando come ottenere *anonimato* e *riservatezza* utilizzando la crittografia end-to-end all'interno di Tails con un'identità contestuale. Nonostante ciò quello che ci interessa potrebbe essere *il solo anonimato o pseudonimato*, senza la riservatezza. In effetti potremmo voler nascondere chi siamo senza necessariamente voler nascondere anche il contenuto delle nostre conversazioni, ad esempio se stiamo discutendo in "stanze" pubbliche che discutono sulle pratiche sessuali considerate devianti. Per seguire questa

16 Cap. 7
17 Tomo I, cap. 14
18 Tomo I, cap 13
19 Tomo I, cap. 14.5.1
20 Cap. 20

ricetta[21] avvieremo Tails e poi utilizzeremo Pidgin[22] con un account creato automaticamente per l'occasione[23] *senza* utilizzare la crittografia end-to-end.
[NdT: *Da quando è stata pubblicata l'edizione originale della Guida, alcune cose sono cambiate (in meglio!). Per le chat di gruppo, molti-a-molti, adesso invece di OTR si può utilizzare OMEMO Multi-End Message and Object Encryption*[24]*. Questo plugin non è supportato da Pidgin, ma lo è da molti altri programmi, come ad esempio Gajim*[25].]

## 11.4 Limiti

Anzitutto, questo metodo resta vulnerabile agli eventuali attacchi alla crittografia di cui parleremo e agli attacchi a Tor[26]. Ma ci sono anche alcuni limiti specifici delle conversazioni in tempo reale. Per esempio, lo stato "online" o "offline" di un'identità in generale è accessibile pubblicamente. Un avversario può anche vedere quando un'identità è connessa ed eventualmente mettere in relazione varie identità: nel caso in cui siano sempre online contemporaneamente o al contrario non siano mai online nello stesso tempo, ma si susseguano spesso, ecc.

*Per fare in modo che delle identità appaiano come "sempre online", è possibile utilizzare un "ghost" o un proxy*[27] *su un computer di cui ci fidiamo, che sia sempre acceso e connesso al server di messaggistica istantanea. In questo modo sarà*

21 Tomo I, cap. 14.1
22 Cap. 20
23 Durante l'avvio di Tails, vengono generati in automatico due account di messaggistica istantanea [busira.vado.li].
24 Wikipedia, *Omemo* [NdT].
25 Wikipedia, *Gajim* [NdT].
26 Cap. 8.3.3
27 Wikipedia, *Proxy*.

*questo computer, e non il server, a "vedere" quando ci si connette, e questo stato non sarà più pubblico. Per il momento però lo sviluppo di una struttura del genere va oltre lo scopo di questa guida.*

Nel caso particolare in cui l'anonimato (o lo pseudonimato) sia prioritario rispetto al resto, per esempio quando vogliamo discutere in una stanza pubblica, si aggiungono altri limiti a quelli già elencati sopra. Un'identità contestuale rischia sempre di venire collegata a un'identità civile, come abbiamo visto nella parte sugli pseudonimi[28]. In effetti, anche sotto pseudonimo, il contenuto e la forma delle nostre conversazioni possono dire moltissimo sulla persona che sta dietro alla tastiera. È importante ricordare che quando proviamo a definire una policy di sicurezza durante una relazione tra più persone, al telefono, via email[29] o attraverso messaggistica istantanea, il livello globale della sicurezza si abbasserà a quello della persona che ha preso meno precauzioni. Per esempio quando decidiamo di utilizzare Tails per non lasciare traccia sul computer, se il nostro interlocutore utilizza invece il suo sistema operativo abituale senza nessuna protezione particolare, diventerà il punto debole di tutta la nostra policy di sicurezza.

---

28 Cap. 5.2
29 Cap. 10

# 12 | Caso d'impiego: condividere documenti sensibili

## 12.1 Contesto

In uno dei casi d'impiego precedenti[1] abbiamo visto come condividere dei documenti che vogliamo rendere pubblici. Ma talvolta è invece necessario condividere con un gruppo ristretto di persone dei documenti sensibili[2] come ad esempio dei documenti di lavoro riservati, delle foto delle vacanze o il contatto di una fonte che vuole divulgare dei documenti aziendali.
Il caso generale esula un po' dal contesto di questa guida; affronteremo invece la condivisione di documenti sensibili via internet, riguardo alla quale potremmo trovare alcune risposte tecniche in queste pagine.

## 12.2 Valutare i rischi

### 12.2.1 Che cosa vogliamo proteggere?

Il contenuto dei file condivisi in questo caso è riservato. Soltanto i destinatari devono potervi accedere, come nel caso di una email esaminato in precedenza[3]. Per esempio, se vogliamo condividere le foto delle vacanze con la nostra famiglia, quello che vogliamo proteggere sono le foto stesse. Il fatto che i destinatari siano i membri della famiglia non è un'informazione sensibile, a priori. Si tratta insomma di *proteggere i contenuti che vogliamo condividere.*
In altri casi, anche chi sta condividendo con chi potrebbe far

1 Cap. 9
2 Tomo I, cap. 9
3 Cap. 10.2.1

parte delle informazioni che vogliamo proteggere. Per riprendere l'esempio precedente, se la cerchia familiare non è un'informazione riservata, sapere chi sta condividendo dei documenti aziendali riservati con chi, lo è molto di più. In questo caso si tratta di *proteggere chi sta condividendo con chi.*
Infine, possiamo voler nascondere i collegamenti tra questi documenti e noi stessi, quando la fonte siamo noi. Una problematica che si pone per esempio, quando si devono diffondere dei documenti sensibili dell'azienda nella quale lavoriamo. In questo caso dobbiamo fare riferimento al caso d'impiego "pubblicare un documento"[4].

### 12.2.2 Da chi vogliamo proteggerci?

Come nel caso d'impiego "visitare siti web"[5], qui cerchiamo di proteggerci dagli sguardi indiscreti che cercano di sapere cosa facciamo sul web. Ma anche da quegli sguardi che potrebbero incappare per caso su questi documenti.

## 12.3 Due problematiche

Un po' come per il caso d'impiego "scambiarsi messaggi"[6], dobbiamo separare la questione in due parti.
La prima riguarda la protezione della fonte e dei destinatari dei documenti. La seconda concerne specificatamente la riservatezza dei documenti da condividere.

4 Cap. 9
5 Cap. 8
6 Cap. 10

## 12.4 Proteggere la fonte

Prima di pensare a come proteggere le differenti persone con cui stiamo condividendo i documenti, dobbiamo assicurarci di non mettere in pericolo noi stessi condividendoli.
Essendo questi documenti confidenziali, in genere non si vuole renderne pubblico il contenuto. Detto ciò, niente ci garantisce che non finirà con l'esserlo, che sia per un errore nostro o delle persone che ci accederanno, o per via di avversari capaci di mettere in crisi la nostra strategia o la sua realizzazione.
Il procedimento sarà molto simile a quello della pubblicazione di un documento[7] che dobbiamo poter leggere o rileggere, però è necessario dare qualche ragguaglio specifico.

### 12.4.1 Prima strategia d'attacco: sta scritto in basso a destra

Se vogliamo condividere dei documenti riservati, tanto più se siamo noi ad averli prodotti, niente ci assicura a priori che ci si possa fidare delle persone con cui li stiamo condividendo.
Immaginiamoci per esempio di voler far vedere i bilanci creativi del nostro partito a un giornalista in modo che ci scriva un articolo senza però renderli pubblici. Di base non abbiamo nessuna fiducia in questo giornalista e preferiamo quindi che non sappia da chi provengono.
Dovremo quindi evitare di lasciarci sopra delle tracce che riconducano a noi. Sia tracce evidenti come delle anagrafiche, sia quelle più discrete, come i metadati[8]. Tutto il lavoro di produzione dei documenti dovrà quindi essere realizzato in un ambiente adatto[9].

---

7 Cap. 9.3
8 Tomo I, cap. 2.6
9 Tomo I, cap. 9

### 12.4.2 Seconda strategia di attacco: mettersi in mezzo

Riprendendo l'esempio precedente, ovvero il caso in cui non ci fidiamo delle persone con cui stiamo condividendo un documento, queste potrebbero, volontariamente o sotto minaccia, rivelare il sito in cui l'hanno trovato.
Da qui, sarebbe relativamente facile, attraverso i log[10] o con una richiesta legale[11] nel caso in cui l'avversario possa farlo, sapere da dove arriva la connessione che ha caricato online quel documento, e di conseguenza risalire al nostro computer.
Per evitare che i diversi intermediari che si trovano tra il nostro computer e il server sul quale è ospitato il documento si dimostrino indiscreti, utilizzeremo la rete Tor[12], attraverso il Tor Browser[13].
Una soluzione alternativa e più radicale è quella di non condividere i nostri documenti adoperando un server terzo, ma usando come server il nostro computer. Questa soluzione permette di configurare sul nostro computer un Onion Service di Tor[14], come spiegato nello strumento "usare OnionShare"[15]. In questo caso, anche se venisse rivelato l'indirizzo web dove si trovano i documenti, ciò non basterebbe a risalire a noi.
Infine, come spiegato nell'introduzione di questo capitolo, in certe situazioni è comunque possibile condividere dei documenti riservati senza doverli far transitare attraverso internet. Questo ci salva dagli intermediari di cui sopra, ma ci lascia con tante altre questioni che riguardano la policy di sicurezza da mettere in atto.

---

10 Cap. 3.2.2
11 Cap. 3.2.4
12 Cap. 7
13 Cap. 14
14 Cap. 7.1.3
15 Cap. 22

### 12.4.3 Terza strategia d'attacco: cercare sul computer della fonte

Sul nostro computer possiamo lasciare, di proposito o no, i documenti riservati o delle tracce di essi.
Questa situazione è la stessa di cui parliamo nel caso d'impiego precedente[16]. Le soluzioni sono quelle di cifrare il proprio hard-disk[17] o di evitare in partenza di lasciare tracce, utilizzando un sistema live amnesico[18].

### 12.4.4 Quarta strategia d'attacco: attaccare Tor

Infine, l'avversario potrebbe anche cercare di attaccare Tor: la sezione "attaccare Tor"[19], contenuta nel primo caso d'impiego, analizza nel dettaglio questa eventualità.

## 12.5 Proteggere i destinatari

Dopo aver preso le precauzioni necessarie a proteggere noi stessi, dobbiamo preoccuparci dei destinatari dei nostri documenti. Anche se non possiamo avere la lista completa delle persone che avranno accesso ai documenti, né impostare una difesa al posto loro, possiamo almeno fare in modo che per accedervi sia necessario mettere in atto un minimo di protezione.
Il modo più semplice, efficace e realizzabile, è quello di utilizzare un Onion Service di Tor[20], che costringerà i destinatari

16 Cap. 12.4.2
17 Tomo I, cap. 15
18 Tomo I, cap. 14
19 Cap. 8.3.3
20 Cap. 7.1.3

a utilizzare anche loro la rete Tor. Per farlo basta seguire lo strumento OnionShare[21].

## 12.6 Proteggere i documenti riservati

Dopo aver pensato a proteggere le persone con cui stiamo condividendo i documenti, non resta che proteggere i documenti stessi.
Il procedimento in questo caso è simile a quello per lo scambio di email confidenziali. Ma non utilizzeremo la posta elettronica, sia perché i documenti potrebbero essere troppo pesanti, sia perché potremmo non avere una lista precisa dei destinatari a cui inviarli. Per questi motivi preferiamo condividere dei file online su un server, come nel caso della pubblicazione[22], ma questa volta in forma privata. Vogliamo dunque nascondere il contenuto di un documento, per esempio una mappa che indica dove è nascosto il nostro tesoro.
Per avere più dettagli sulle differenti fasi della nostra policy di sicurezza, andiamo a rivedere cosa abbiamo detto riguardo allo scambio di email riservate[23].
Le soluzioni utilizzate comportano tutte la cifratura[24], sebbene sotto aspetti differenti a seconda della nostra policy di sicurezza e della nostra ottica di condivisione.

### 12.6.1 Scegliere tra gli strumenti disponibili

Esistono vari strumenti per cifrare i nostri file prima di condividerli. La scelta dell'uno o dell'altro dipende soprattutto

21 Cap. 22
22 Cap. 9
23 Cap. 10.8
24 Tomo I, cap. 5.1

dal livello di condivisione e dalla qualità della cifratura desiderata.

### 12.6.2 Cifratura online

Innanzitutto, la soluzione più economica in termini di energie è quella di mettere i nostri documenti su un servizio di file server[25], che si occuperà di cifrare automaticamente i file sul server in cui verranno ospitati.
Per questa strategia bisogna scegliere un servizio del quale ci fidiamo, perché sarà esso ad occuparsi della cifratura. Inoltre potrebbe ricevere delle pressioni o richieste legali[26] da parte delle guardie, che lo potrebbero obbligare a decifrare i file archiviati, sempre che sia tecnicamente possibile farlo. Anche se permette effettivamente ai nostri documenti di non essere accessibili pubblicamente, la cifratura online non garantisce la riservatezza contro degli avversari attivi.
Se vogliamo lo stesso scegliere la cifratura online, possiamo ispirarci alla sezione corrispondente nello strumento "scegliere un servizio di hosting"[27].

### 12.6.3 Cifratura offline

Un'altra possibilità è quella di cifrare direttamente il documento prima di metterlo online. Questa soluzione è un po' più complessa da mettere in campo, ma ha come vantaggio quello di non esigere un'elevata fiducia in un'entità terza: sceglieremo da soli come cifrare i nostri file.
Ancora una volta sono disponibili molte opzioni. Potremo ci-

---

25 Cap. 15
26 Cap. 3.2.4
27 Cap. 15

frare i nostri documento con una passphrase[28], o attraverso una o più chiavi pubbliche[29], a seconda dei diversi destinatari. In entrambi i casi, dobbiamo prestare attenzione al nome della cartella che contiene i documenti cifrati: se il nome è esplicito, può rivelare informazioni sul contenuto dei documenti. Chiamiamo la cartella con un nome neutro, "documenti" o "archivio".

### Cifrare con una passphrase

Cifrare i nostri file con una passphrase permette a chiunque la possieda di decifrarli e avere accesso ai documenti. Dovrà però sapere anche dove trovarli: necessiterà dell'indirizzo web per scaricarli oppure di avere accesso a uno dei computer sul quale sono salvati.
Un dettaglio da non sottovalutare è che chiunque abbia accesso ai file deve conoscere la passphrase. Dobbiamo quindi usare un mezzo di comunicazione riservato per condividere questo segreto con tutte le persone destinatarie, cosa che potrebbe non essere semplice.
Infine ci si presenteranno gli stessi limiti invocati nel capitolo sulla crittografia simmetrica[30].
Per utilizzare questo metodo occorre seguire la ricetta "cifrare dei dati"[31], e poi scegliere una delle due soluzioni invocate prima per ospitare questi documenti: un servizio di hosting web[32], o ospitarli da noi stessi attraverso OnionShare .

### Cifrare con una o più chiavi pubbliche

Nel caso in cui abbiamo un elenco definito di persone con cui condividere i documenti e ciascuna di esse possiede una

28 Tomo I, cap. 12
29 Cap. 6.2.1
30 Cap. 6.1
31 Cap. 19.12
32 Cap. 15

coppia di chiavi OpenPGP, possiamo cifrare i file con le loro chiavi in modo che solo loro riescano a decifrarli.
Anche in questo caso dobbiamo seguire la ricetta “cifrare dei dati” , e poi scegliere una delle due soluzioni invocate prima per ospitare questi documenti: un servizio di hosting web , o ospitarli da noi stessi attraverso OnionShare[33].

**Decifrare i file**
I destinatari dei documenti potranno decifrarli seguendo la relativa ricetta[34].

33 Cap. 22
34 Cap. 19.13

TERZA PARTE

# Strumenti

In questa terza parte spiegheremo come applicare concretamente alcune delle strade sopra menzionate.
Questa parte è solo un'appendice tecnica alle precedenti: una volta comprese le problematiche legate all'intimità nel mondo digitale; una volta scelte le risposte appropriate, resta la domanda "Come si fa?", a cui questa appendice fornisce alcune risposte.

**Circa il buon uso delle ricette**
Gli utensili e le ricette che seguono sono soluzioni estremamente limitate, inutili se non inquadrate in un insieme coerente di pratiche. Pescare da questa cassetta degli attrezzi senza aver studiato in precedenza la sezione sulla scelta di una risposta appropriata[1] e sulla definizione di una policy di sicurezza[2], è un ottimo modo per tirarsi la zappa sui piedi credendo, erroneamente, di aver risolto questo o quel problema.

**Non possiamo accontentare tutti**
Per la maggior parte delle ricette contenute in questa guida, abbiamo dato per scontato che si stia usando GNU/Linux con il Desktop GNOME; queste ricette sono state scritte e testate sotto Debian 9.0 (chiamata Stretch[3])e Tails[4] (The Amnesic Incognito Live System). Tuttavia, queste sono generalmente adattabili ad altre distribuzioni basate su Debian, come Ubuntu[5] o LinuxMint[6]. Se non stiamo ancora usando GNU/Linux, possiamo consultare i casi d'uso del primo volume, nel capitolo "Un nuovo inizio"[7] o "Utilizzare un sistema live"[8].

1 Parte seconda
2 Cap. 7
3 https://www.debian.org/releases/stretch/
4 https://tails.boum.org/
5 https://www.ubuntu-it.org/
6 https://linuxmint.com/
7 Tomo I, cap. 8
8 Tomo I, cap. 14

**Sulla corretta interpretazione delle ricette**

Prima di passare alle ricette stesse, ci sembra necessario fare alcune osservazioni trasversali.

Le procedure sono presentate passo passo e spiegano, quando possibile, il significato delle azioni che ci proponiamo di compiere. Un uso efficace di questi strumenti richiede un accordo su alcuni punti:

- L'ordine in cui viene sviluppata ogni ricetta è della massima importanza. Salvo diversa indicazione, è semplicemente inimmaginabile saltare un passaggio per poi recuperarlo in seguito: il risultato, se mai queste operazioni disordinate dovessero darne uno, potrebbe essere molto diverso dal previsto, o semplicemente catastrofico.
- Allo stesso modo, le azioni indicate devono essere eseguite alla lettera. L'omissione di un'opzione o l'apertura del file sbagliato può avere l'effetto di cambiare completamente il risultato ottenuto rispetto a quello atteso.
- In generale, una buona comprensione di queste ricette richiede la concessione un minimo di attenzione e vigilanza. Non possiamo spiegare tutto a ogni volta: si dà implicito l'aver preventivamente consultato e compreso le spiegazioni dei "casi d'impiego"[9], di cui queste ricette sono solo l'ultimo passaggio.
- Infine, i software si evolvono in fretta, motivo per cui si consiglia vivamente di utilizzare il versione più aggiornata di questa guida, disponibile sui siti `https://guide.boum.org/` e `https://numerique.noblogs.org/`.

---

9 Parte seconda

# 13 | Installare e configurare Tor Browser

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da mezz'ora a un'ora

Abbiamo visto che, durante la nostra navigazione sul web, i siti visitati possono registrare il nostro indirizzo IP[1] e attraverso di esso un avversario può poi facilmente risalire a noi. Da qui, a volte, la necessità di nascondere questo indirizzo IP. Tor è un software che permette alla nostra connessione di passare attraverso una rete di "nodi", chiamati relay, mascherando così il nostro vero IP. Questo sistema viene chiamato onion routing[2].
Per poter usare la rete di anonimizzazione Tor, è necessario configurare il software Tor stesso, ma anche il software che lo utilizzerà, come ad esempio il browser web. Queste impostazioni sono spesso complesse, a tal punto che è difficile essere sicuri dell'anonimato che ne risulta.
Ecco perché è consigliabile, per utilizzare Tor, di servirsi o di un sistema live[3] dedicato a questo uso, o di utilizzare un "kit pronto all'uso": il Tor Browser è uno strumento che rende molto facile l'installazione e l'utilizzo di Tor su un sistema "classico". Non sarà necessaria alcuna configurazione e tutti i software indispensabili per navigare con Tor sono inclusi.

1 Cap. 1.2.5
2 Cap. 7.1
3 Tomo I, cap. 14

Il Tor Browser riunisce:

- il browser web Firefox, configurato per utilizzare Tor;
- il software Tor;
- un launcher, per avviare il tutto con un semplice doppio clic.

⚠ *Attenzione*: va tenuto presente che Tor Browser non fornisce l'anonimato per l'intero computer: solo le connessioni ai siti web che utilizzano questo browser passano attraverso Tor. *Tutte le altre connessioni (client di posta, aggregatori di feed RSS, Torrent, altri browser, ecc.) non sono anonime.* Inoltre, le tracce di navigazione, come cookie o passphrase, verranno probabilmente salvate sul disco rigido, così come i documenti scaricati. Infine, capita a volte che durante la navigazione si faccia clic su un collegamento che avvia automaticamente un software (ad esempio un lettore musicale) che *non* passerà attraverso Tor. Degli indizi sulla natura della nostra navigazione potrebbero insomma trapelare comunque.

Qui spiegheremo come installare Tor Browser su una Debian cifrata[4].
Per utilizzare un sistema che si connette a internet unicamente tramite Tor e per poter utilizzare Tor con un software diverso da un browser, servirà ricorrere a un sistema live[5] come Tails.

## 13.1 Scaricare e controllare Tor Browser

NdT: Nella versione originale della Guida, la procedura per installare Tor Browser era abbastanza più impegnativa e richiedeva diversi passaggi: era il metodo più sensato in quel

4 Tomo I, cap. 15
5 Tomo I, cap. 14

momento. Al momento in cui scriviamo, esiste un metodo decisamente più comodo e altrettanto sicuro: installare il pacchetto Debian Tor Browser Launcher e seguire la procedura guidata. Abbiamo quindi scelto di riscrivere questo capitolo, sostituendo le vecchie istruzioni con quelle nuove più aggiornate.

### 13.1.2 Installare Tor Browser Launcher

I consigli dettagliati su come scegliere, verificare e installare un programma possiamo trovarli sul primo volume di questa guida[6]. Procediamo quindi come prima cosa installando il pacchetto `torbrowser-launcher`.
Una volta installato, lanciamolo cliccando su ⊞ (⌘ su Mac), scriviamo `tor` e poi clicchiamo su "Tor Browser". Al primo utilizzo Tor Browser Launcher si occuperà come prima cosa di scaricare il programma Tor Browser: si aprirà una finestra che mostra le fasi di avanzamento del download e dell'installazione. Tor Browser Launcher si occuperà anche di scaricare e verificare la firma del software di Tor Browser: in questo modo ne avremo verificato l'autenticità
Una volta finito verrà lanciato Tor Browser e ci troveremo per la prima volta davanti al nostro programma. La finestra di Tor Browser, una volta lanciato, ci proporrà ogni volta sia di connettersi alla rete Tor direttamente ("Connect"), sia di configurarla ("Tor Network Settings"). Per iniziare clicchiamo su "Connect" e aspettiamo che il programma si connetta per la prima volta alla rete Tor.
Può accadere in determinate condizioni, come il blocco delle connessioni alla rete Tor da parte dei fornitori di servizi internet, che Tor Browser non riesca a connettersi. In questo caso, o semplicemente per maggiori informazioni, consultare la do-

6 Tomo I, cap. 16

cumentazione disponibile sul sito del progetto Tails.
Se invece è andato tutto bene, abbiamo finito la nostra procedura di installazione e possiamo iniziare a navigare utilizzando la finestra del Tor Browser.

# 14 | Navigare in rete con Tor

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: 5-10 minuti.

Questa ricetta serve a navigare sul web in modo anonimo utilizzando Tor[1]. Non ci sono molte differenze tra l'utilizzo di un browser "classico", che diamo per scontato si sappia usare. La documentazione di Tails riguardo al NetworkManager ci spiegherà come collegare il nostro computer a internet.

## 14.1 Avviare il browser

Se non stiamo utilizzando il sistema live Tails[2], dovremo installare Tor Browser[3].
Attenzione, quando utilizziamo Tor Browser solo la navigazione che effettueremo tramite di esso beneficerà dell'anonimato di Tor.

## 14.2 Qualche avvertenza sulla navigazione

Una volta lanciato lo si può usare praticamente come un normale browser. Ci sono però dei dettagli a cui fare attenzione.

1 Cap. 7
2 Tomo I, cap. 14
3 Cap. 13

Innanzitutto dobbiamo aver capito bene da cosa ci protegge Tor, ma soprattutto da cosa non ci protegge affatto[4], in modo da non fare questo e quello credendosi al sicuro.
Oltre a questi limiti, dobbiamo sapere che i siti che consultiamo possono accorgersi che ci stiamo connettendo tramite la rete Tor. Alcuni, come Wikipedia, lo fanno per evitare la pubblicazione anonima. Altri, come Google, prima di farci accedere ai loro servizi ci chiederanno di risolvere alcuni quiz chiamati “captcha”[5] per essere certi che siamo umani.
Infine, su Tor Browser alcune funzionalità vengono disattivate per proteggere l’anonimato. Ad esempio Flash[6], una tecnologia utilizzata da molti siti che offrono video in streaming.

4 Cap. 7.3
5 Wikipedia, *Captcha*.
6 Cap. 2.1.3

# 15 | Scegliere un servizio di hosting

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da mezz'ora a un'ora.

L'obiettivo di questa ricetta è quello di trovare dove far ospitare un documento sul web. Le possibilità sono troppe per poter dare una risposta "chiavi in mano" e inoltre consigliare un piccolo elenco di servizi di hosting, sui quali verrebbero quindi centralizzati molti contenuti "a rischio", non ci sembra una buona idea. Daremo quindi piuttosto qualche consiglio sui criteri per fare una buona scelta.
È anche possibile ospitarsi da soli[1] il proprio documento, in modo anonimo, utilizzando gli Onion Service di Tor[2]. Per farlo potete consultare la ricetta circa l'utilizzo di OnionShare[3].

## 15.1 Criteri

Esistono talmente tanti servizi di hosting che ben presto potremmo sentirci persi nella giungla delle possibilità. Ecco qualche criterio per porsi le giuste domande. Di seguito parleremo di documento, ma questi criteri valgono anche per oggetti più ambiziosi e pesanti, come un blog o un documentario video.

1 Cap. 4.5
2 Cap. 7.1.3
3 Cap. 22

- **Tipo di organizzazione**: molti siti offrono hosting "gratuito". Molti di questi sono servizi commerciali che hanno un interesse a pubblicare contenuti creati dai loro utenti[4]. Esistono però anche associazioni o collettivi che ospitano progetti a determinate condizioni.
- **Condizioni**: : se il documento non è gradito a chi lo ospita, nulla gli impedisce di farlo sparire senza neanche avvisarci. Le condizioni di utilizzo (che ci viene chiesto di accettare per ospitare il nostro documento) spesso ci danno un'idea di cosa viene tollerato o no.
- **Resistenza alle pressioni**: lo Stato potrebbe voler oscurare il nostro documento. In molti casi gli basta intimidire il servizio di hosting per ottenere che lo cancelli. I diversi servizi reagiscono in modo differente alle pressioni: alcuni aspettano un procedimento legale, altri cancellano tutto subito alla prima email vagamente minacciosa.
- **Cancellazione del documento**: al contrario, potremmo voler cancellare il nostro documento. Essendo l'hosting un servizio che deleghiamo ad altre persone più o meno fidate, non possiamo avere la certezza che i nostri file vengano davvero cancellati. Conoscere chi ci ospita in certi casi può darci più garanzie.
- **Rischi per chi ci ospita**: a seconda del contenuto del nostro documento, la sua pubblicazione potrebbe far correre dei rischi a chi lo ospita, in particolare se si tratta di un servizio di hosting che non ha l'abitudine di collaborare con le guardie. In questo caso dobbiamo chiederci se siamo pronti a far correre questo rischio a chi ci ospita, considerando che potrebbe anche essere costretto a chiudere spinto dalla repressione.
- **Dimensioni del documento**: se il nostro documento è "troppo grande", certi servizi di hosting si rifiutano di ac-

4 Cap. 4.2

cettarli. La stessa cosa potrebbe succedere anche se il documento fosse "troppo piccolo". Alcune offerte specificano le dimensioni consentite, ma attenzione: alcuni servizi mettono a pagamento alcune funzionalità come l'hosting di file molto grandi.

- **Durata dell'hosting**: la durata dell'hosting varia molto di offerta in offerta. Per esempio alcuni cancellano automaticamente il documento dopo un certo periodo di tempo, altri se non viene scaricato entro una certa data, ecc.

## 15.2 Tipo di contenuto

Adesso che abbiamo un po' chiarito le idee sui criteri di scelta, proviamo a scendere più nel concreto. Il servizio di hosting adatto al nostro progetto dipende innanzitutto dal tipo di contenuto che vogliamo pubblicare: un testo, un'immagine, un video, un audio, ecc.

### 15.2.1 Pubblicare un testo

Pubblicare un testo spesso è la cosa più semplice.
Se il testo da pubblicare è in relazione a un altro già pubblicato, spesso basta mettere un commento, che si tratti di un blog, un forum o un qualche altro sito partecipativo. Per questo tipo di pubblicazione spesso non è obbligatorio registrarsi, ma questo non vuol dire assolutamente che la pubblicazione sia anonima a meno di non prendere precauzioni particolari, come per esempio usare la rete Tor[5]. Inoltre se il nostro testo è un commento, e non un oggetto in primo piano, non è detto che gli venga dato risalto sul sito.

---

5 Cap. 7

Oppure si potrebbe voler pubblicare un testo su un sito o su un blog che già esiste. In questo caso bisognerà mandarlo al sito in questione tramite un form o via email e la pubblicazione dipenderà dagli amministratori. Alcuni siti consentono invece la pubblicazione libera di articoli su un determinato tema.

### 15.2.2 Pubblicare un blog o un sito

Se vogliamo pubblicare regolarmente dei testi, possiamo scegliere di amministrare un blog: ci sono molte organizzazioni che offrono blog già configurati e facili da usare. Altrimenti possiamo anche amministrare un sito web, questo richiede però un po' di gavetta in più. In molte città ci sono gruppi di persone che si interessano al software libero o alla libertà d'espressione su internet e che potrebbero darci buoni consigli. Ci sono alcune liste disponibili anche sul web:

- un elenco di alcune grandi piattaforme di blog, su Wikipedia: `rimale.vado.li`;
- una lista di servizi web liberi sul wiki della comunità francofona di Ubuntu: `ritenu.vado.li`;
- esiste anche noblogs.org: `https://noblogs.org`.

### 15.2.3 Pubblicare file audiovisivi

Per pubblicare immagini, video, o audio, per esempio in accompagnamento al testo di un articolo, ci sono diverse soluzioni. Per la verità, la maggior parte dei siti in cui è possibile pubblicare un testo offre anche di poter allegare dei documenti audio/video. Questi siti permettono anche di scegliere se prendere i file dal nostro computer (che verranno poi ospitati

sui loro server), o se indicargli il link dove i file sono già ospitati altrove.
Esistono anche alcuni siti di condivisione o file hosting. Eccone qualcuno:

- Il progetto Framasoft è consacrato principalmente all'universo del software libero e offre gratuitamente diversi strumenti, in particolare Framadrop per la condivisione dei file e Framapic per l'hosting delle immagini. Questi servizi hanno il vantaggio di tenere cifrati i file sui propri server[6].
- Internet Archive, un'organizzazione senza scopo di lucro, nasce per essere una biblioteca digitale libera.

Con lo stesso spirito dei progetti di archivistica, condivisione o hosting di file e servizi, ha visto recentemente la luce un'iniziativa che si chiama CHATONS: Collectif d'Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires (Collettivo di Hosting Alternativo, Trasparente, Aperto, Neutro e Solidale).
Questo collettivo ha come obiettivo quello di raggruppare le organizzazioni (francesi, NdT) che offrono servizi rispettosi della vita privata dei loro utenti.

### 15.2.4 Pubblicare un file scaricabile di grosse dimensioni

Per pubblicare dei documenti che vogliamo possano essere scaricati, dobbiamo cercare tra i servizi di DDL (Direct Download Link).
Carichiamo il file direttamente sul server e otteniamo un link che se incollato nel browser fa partire lo scaricamento del file.

---

6 Framasoft ha recentemente chiuso questi servizi, ma se ci andate troverete comunque un elenco di servizi alternativi consigliati [NdT].

Alcuni di questi servizi:

- Lista su Wikibooks di alcuni siti di condivisione file: `zamomi.vado.li`;
- [NdT: Un elenco di strumenti utili, per certi versi più aggiornato e ampio, lo possiamo trovare sul sito dell'hacklab fiorentino If_Do `https://ifdo.noblogs.org/strumenti/`. Come si legge nella pagina, si tratta di una: "raccolta di strumenti utili, non commerciali, autogestiti e rispettosi della vostra intimità"].

## 15.3 In pratica

Come prima cosa scegliamo il servizio di file hosting: i criteri che abbiamo raccolto precedentemente dovrebbero aiutarci nella scelta. È molto importante scegliere un servizio di cui ci fidiamo veramente perché il nostro anonimato potrebbe dipendere in parte da questa scelta.
È anche possibile cifrare[7] i file che vogliamo ospitare. Per farlo ci sono due possibilità, possiamo cifrarlo prima di caricarlo[8] oppure scegliere un servizio di hosting che cifrerà il file sui propri server (come nel caso di `https://zerbino.esiliati.org/`, NdT). In seguito dobbiamo capire come caricare nel concreto il file. I metodi variano a seconda del servizio, ma il principio resta lo stesso. Per prima cosa apriamo il browser e usiamolo in modalità anonima[9]. Andiamo sulla pagina del servizio di file hosting e troviamo dove "caricare" (upload in inglese) il nostro file. Da qui dobbiamo seguire le istruzioni specifiche di ciascun servizio. In generale, si tratta di un'operazione piuttosto semplice e anche se possono esserci delle differenze, resta simile su qualunque servizio. Una volta finito l'upload ci verrà

7 Cap. 12.6.1
8 Cap. 19.1
9 Cap. 8

mostrato l'indirizzo web al quale si trova il file.
A volte può essere necessario inserire un indirizzo email per ricevere questo link: per decidere quale indirizzo usare, seguiamo il caso d'impiego sullo scambio di email[10] e il capitolo sulle identità contestuali[11].
Una volta ottenuto il link, possiamo condividerlo nel modo che ci sembra migliore. Chi dispone di quel link potrà scaricarsi il file inserendolo nella barra degli indirizzi del browser.

10 Cap. 10.7.1
11 Cap. 5

# 16 | Verificare un certificato

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 15 a 30 minuti.

Abbiamo visto nella prima parte di questa guida, che per stabilire una connessione cifrata dobbiamo spesso fare affidamento su una Certification Authority (CA)[1]. Nella maggior parte dei casi le CA sono già registrate sul computer, per esempio nel browser. Ma non è sempre così: nel caso che prenderemo in esame ora, il nostro browser o un altro programma ci presenterà un messaggio che dirà di non essere stato in grado di autenticare il certificato di un determinato sito.
Può anche succedere che, non fidandosi delle CA, il sito che stiamo visitando non utilizzi i servizi di una Certification Authority. E allora dovremo verificare noi il suo certificato.

## 16.1 Verificare un certificato o una Certification Authority

Sia il certificato di una CA che quello di un singolo sito devono essere verificati prima di accettarli. Senza questo passaggio la connessione sarà pure cifrata, ma non *autenticata*. Come dire, possiamo anche cifrare la comunicazione, ma se non sappiamo chi la sta cifrando[2] siamo lontani dal poterci sentire tranquilli.

---

1 Cap. 6.4.2
2 Cap. 6.4.1

Verificare un certificato significa per la maggior parte delle volte visualizzarne l'hash[3] e confrontarlo con un'altra fonte in modo da assicurarci che sia corretto. Usiamo preferibilmente l'hash di tipo SHA-256 e non quello MD5[4] o SHA-1[5], perché questi ultimi sono ormai considerati insicuri.
Per la Certification Authority Let's Encrypt, per esempio, otterremo una serie di caratteri di questo tipo:

```
48:9F:2D:A9:37:2C:68:4E:31:3E:EA:38:3E:BD:1B:E4:
F1:0C:59:EF:60:BB:EB:0A:FA:78:82:AB:98:E2:E1:DF
```

Nel caso di un sito web, per avere accesso all'hash di un certificato, quando andiamo su un indirizzo che comincia per "https" otterremo un messaggio di avviso simile a questo:

> **Connessione sicura non riuscita**
> Si è verificato un errore nella configurazione di *sito.com.*
> Per evitare rischi per la sicurezza dei vostri dati, Tor Browser non si connetterà a questo sito.
> Ulteriori informazioni...
> *Torna indietro*
> *Avanzate*

I "rischi per la sicurezza" a cui si riferisce l'avviso sono stati affrontati in un capitolo nella prima parte della guida[6]. Una volta letto l'avviso possiamo cliccare su "Avanzate", che farà comparire il messaggio seguente:

3 Tomo I, cap. 5.2
4 Chad R Dougherty, 2008, *MD5 vulnerable to collision attacks* [gevola.vado.li].
5 Julien Cadot, 2017, *SHAttered: Google a cassé la fonction de hachage SHA-1* [forafi.vado.li].
6 Cap. 6.4.1

> sito.com uses an invalid security certificate.
> The certificate is only valid for the following names: dominio.org, dominio.org
> Error code: SSL_ERROR_BAD_CERT_DOMAIN
> *Aggiungi un'eccezione...*

Clicchiamo su "Aggiungi un'eccezione...".
Si aprirà una finestra per l'aggiunta dell'eccezione di sicurezza. In questa finestra, sotto "Stato del Certificato", possiamo trovare delle informazioni interessanti sul motivo per cui il browser non ha voluto accettare il certificato.
Nel caso di un certificato autofirmato, per esempio, leggeremo una frase del tipo "Questo sito ha cercato di identificarsi con delle informazioni non valide". Può essere successo ad esempio che la data della validità del certificato sia scaduta, il che non ne impedisce necessariamente l'utilizzo. In ogni caso è sempre utile leggere questa parte e chiedersi se, dopo queste informazioni, vogliamo comunque continuare. Clicchiamo su "Visualizza..." e poi su "Dettagli", in questo modo possiamo guardare approfonditamente il certificato e capire per esempio da chi è stato emesso, per quanto tempo è valido, ecc.
Torniamo poi a "Generale" e troveremo diverse informazioni sul certificato, tra cui l'hash SHA1.
Adesso non ci resta che cercare un'altra fonte che ci permetta di visualizzare questo hash. Ci sono alcune tecniche per provare ad assicurarci dell'autenticità del certificato:

- Se una persona vicina a noi di cui ci fidiamo utilizza già il sito o la CA in questione e ha già verificato il suo certificato, possiamo confrontare l'hash del suo certificato con quello che abbiamo noi. Per maggiore sicurezza possiamo anche chiedere che ce lo mandino per email in modo cifrato *e autenticato*. Ancora meglio se conosciamo più persone, magari che utilizzano connessioni internet diverse. Per trovare un certificato già installato sul browser

di qualcuno, seguiamo la spiegazione che troveremo nelle prossime righe.

- Se abbiamo accesso a diverse connessioni internet nel posto in cui ci troviamo, per esempio in una città dove ci sono a disposizione diversi accessi wi-fi, visitiamo il sito o scarichiamo il certificato della CA attraverso varie di queste connessioni e confrontiamo gli hash del certificato che via via ci verranno proposti.
- Se stiamo utilizzando il Tor Browser, possiamo approfittare del cambio di circuito[7] – e quindi dell'exit relay – per verificare a più riprese l'hash del certificato. In questo modo eviteremo che un avversario che ha messo le mani su un exit relay, o che si è riuscito a porre tra l'exit relay e il sito consultato, possa usurparne l'identità[8].

Per sapere se l'exit relay dal quale usciamo è cambiato, dobbiamo visitare con il nostro Tor Browser un sito come `torproject.org`, che ci mostra l'IP del nostro exit relay Ogni volta che questo IP cambia, visitiamo il sito che vogliamo vedere o scarichiamo il certificato della CA e confrontiamo il suo hash con quelli che abbiamo scaricato le volte precedenti. Dopo un po' di tentativi andati a buon fine la possibilità che si tratti realmente del certificato vero è sufficientemente alta da poterlo accettare. Dopodiché sta a noi giudicare, in base alla nostra personale policy di sicurezza[9]!

Queste pratiche che abbiamo descritto, utilizzate singolarmente non sono necessariamente molto robuste, ma il loro utilizzo congiunto porta ragionevolmente a credere che si tratti del certificato giusto. E che nessuno è riuscito a fregarci.

Teniamo presente però che questo non ci protegge da ogni attacco verso la cifratura della connessione[10].

---

7 Cap. 7.1.2

8 Cap. 6.4.1

9 Tomo I, cap. 7

10 Cap. 6.4.2

## 16.2 Trovare l'hash di un certificato già installato

L'hash può essere visualizzato cliccando su ≡, per entrare nel menu del Tor Browser. Scegliamo "Avanzate", poi "Certificati", infine clicchiamo su "Visualizza i certificati". Vedremo i certificati installati cliccando su "Server", poi selezionando dall'elenco il sito in questione e cliccando su "Visualizza". La stessa operazione può essere effettuata per le Certification Authority cliccando su "Authority".

# 17 | Usare una tastiera virtuale su Tails

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: pochi minuti.

Abbiamo visto nel primo volume che un computer può essere manomesso fisicamente. Potrebbe quindi contenere un keylogger[1] hardware che registra tutto quello che digitiamo sulla tastiera. I testi che scriviamo, le azioni che compiamo, ma soprattutto le password che digitiamo.
Se abbiamo dei dubbi sul computer sul quale stiamo utilizzando Tails, possiamo usare una tastiera virtuale per rendere inefficace il recupero di ciò che viene battuto fisicamente sui tasti. Attenzione però che questo non ci protegge da un malware che, per esempio, potrebbe salvarsi le schermate di ciò che facciamo[2].

## 17.1 Usare una tastiera virtuale su Tails

Una tastiera virtuale è un programma che appare come una tastiera e che ci permette di scrivere dei caratteri senza utilizzare la tastiera hardware del computer. Può essere usata tramite vari dispositivi come per esempio un mouse, un touchscreen o un touchpad.
Su Tails è installata di default la tastiera virtuale di GNOME.

1 Tomo I, cap. 3.4
2 Tomo I, cap. 3

Viene lanciata automaticamente al momento dell'avvio di Tails e ci si accede cliccando sulla sua icona "Accesso Universale", nell'area delle notifiche in alto a destra, poi mettiamo a "On" l'opzione "Tastiera a schermo".
Una volta lanciata basta scrivere le password utilizzando il mouse, il touchpad o altri dispositivi simili.

# 18 | Usare il client mail Thunderbird

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 15 a 30 minuti.

Questa parte descrive come configurare il client di posta Thunderbird in modo da poterlo usare per tutte le attività relative alle email.

## 18.1 Installare il client mail Thunderbird

Se stiamo utilizzando una Debian cifrata[1], dobbiamo per prima cosa installare[2] il programma Thunderbird. Per farlo installiamo i pacchetti `thunderbird` e `thunderbird-locale-it`.
Se stiamo utilizzando Tails, sia Thunderbird che i pacchetti necessari alla crittografia delle email sono già installati di default. Se non vogliamo dover riconfigurare Thunderbird ad ogni avvio di Tails, e vogliamo poter conservare le nostre mail, contatti ecc. da una sessione all'altra, dobbiamo attivare in anticipo l'opzione Thunderbird nella persistenza di Tails[3].

1 Tomo I, cap. 15
2 Tomo I, cap. 16.3.1
3 TomoI, cap. 14.5

## 18.2 Lanciare Thunderbird

Una volta installati i pacchetti, lanciamo Thunderbird cliccando il tasto ⊞ (⌘su Mac), scriviamo `thu` e poi clicchiamo su "Email Mozilla Thunderbird".

## 18.3 Configurare un account di posta

Quando lanciamo Thunderbird, se non c'è nessun account di posta configurato, apparirà una finestra per la configurazione dell'account. Su una Debian cifrata la procedura richiede un passaggio in più rispetto a Tails. Se vogliamo aggiungere un account in più a Thunderbird leggiamo direttamente il capitolo "Con la procedura di creazione dell'account" più avanti[4]. Solo sotto Debian appare una finestra che dice: "Si desidera creare un nuovo indirizzo di posta?". Clicchiamo sul tasto "Saltare questo passaggio e utilizzare un indirizzo esistente". La finestra che apparirà a questo punto sarà quella di cui parliamo nel paragrafo seguente. Una finestra ci proporrà la "Creazione di un indirizzo di posta", e ci assisterà nella configurazione del programma e nell'aggiunta di un primo account a partire da un indirizzo di posta già esistente.

### 18.3.1 Con la procedura guidata (primo avvio)

Per configurare un account di posta, riempiamo i tre campi che ci vengono richiesti per la "Creazione nuovo account", poi clicchiamo su "Avanti". Possiamo riempire il campo "Nome completo" con lo pseudonimo che vogliamo appaia nelle intestazioni[5]. La procedura guidata ci proporrà a questo punto

4 Cap. 18.3.2
5 Cap. 2.4.2

di scegliere tra due protocolli, IMAP o POP[6]. Selezioniamo quello che preferiamo e clicchiamo su "Fatto".
Thunderbird è adesso pronto a ricevere messaggi. Se vogliamo aggiungere un altro indirizzo di posta supplementare continuiamo la lettura. Altrimenti passiamo al prossimo capitolo, dedicato alla configurazione avanzata di Thunderbird.

### 18.3.2 Con la procedura di creazione dell'account

Per aggiungere un nuovo indirizzo di posta a Thunderbird clicchiamo su ≡ per visualizzare il menu di Thunderbird e andiamo su "Preferenze" → "Impostazioni account". Poi andiamo sul menu "Azioni account" e scegliamo "Aggiungi account di posta..."
A questo punto si aprirà una finestra "Configura un account email esistente". Da questo punto in poi seguiamo le stesse istruzioni del paragrafo precedente.

## 18.4 Configurazione avanzata di Thunderbird

Una volta configurato un account di posta dentro Thunderbird, potremmo voler ottimizzare la configurazione di tutto il programma, in modo da personalizzarlo o ridurre i rischi in termini di sicurezza informatica.
Scegliamo "Impostazioni account" da dentro il menu "modifica". Non possiamo trattare in modo esaustivo tutte le opzioni di configurazione, ma ne prenderemo in esame qualcuna che ci sembra utile.
Per prima cosa, se abbiamo scelto di utilizzare il protocollo POP, dentro la parte "Impostazioni server" potremo decide-

6 Cap. 1.2.3

re il tempo dopo il quale i messaggi verranno cancellati dal server in seguito all'importazione. Questo non ci dà grandi garanzie e dipende soprattutto dal nostro server di posta: possiamo solo sperare che cancellino veramente i nostri dati[7].
Infine potrebbe essere che le porte del protocollo utilizzato non corrispondano a quelle delle impostazioni di default. In questo caso modifichiamo la porta IMAP o POP dentro la sezione "Impostazioni del server" seguendo i parametri forniti dal nostro server di posta. Per modificare la porta SMTP, bisogna andare nella sezione "Server in uscita" (SMTP), selezionare l'account di posta in questione, cliccare su "Modifica..." e modificare il numero di porta.

### 18.3.2 Configurare la crittografia con OpenPGP

NdT: Nell'edizione originale di questa guida, pubblicata nel 2017, si includono a questo punto le istruzioni su come configurare il plugin Enigmail dentro Thunderbird, che fino a quel momento era il metodo tradizionale con cui veniva implementata la crittografia dentro Thunderbird. L'accoppiata Thunderbird + Enigmail è supportata però fino alla versione 68 di Thunderbird. Dalle versioni successive Thunderbird ha deciso di implementare il supporto a OpenPGP direttamente al suo interno, senza più affidarlo a un plugin come avveniva prima.
Le istruzioni che troverete qui di seguito sono quindi state riscritte da noi traduttrici e traduttori per renderle attuali. Come però del resto viene ripetuto in tutta la guida, i software evolvono molto velocemente, il consiglio che vi diamo è quindi quello di non prendere alla lettera queste istruzioni, ma concentrarvi sul comprendere lo spirito e i meccanismi in generale in modo da potervi poi orientare anche in caso di cambiamenti.

---

7 Tomo I, cap. 4.3

Se vogliamo utilizzare la crittografia asimmetrica, per cifrare delle email, firmarle o entrambe le cose, Thunderbird contiene già al suo interno il sistema per farlo. Come prima cosa dobbiamo dire a Thunderbird quali sono le nostre chiavi, pubblica e privata. Se possediamo già una coppia di chiavi (cfr. capitolo su OpenPGP[8]) possiamo importarle, altrimenti dobbiamo crearci una nuova coppia e possiamo farlo direttamente dentro Thunderbird.
Dentro il menu di Thunderbird ≡ → "Impostazione account" → selezionare il proprio account → "Crittografia End-to-End" → "Aggiungi chiave..."
Se abbiamo già la nostra coppia di chiavi possiamo scegliere "Importa una chiave OpenPGP" esistente, se dobbiamo invece crearne una nuova scegliamo "Crea una nuova chiave OpenPGP". In entrambi i casi poi clicchiamo su "Continua", la configurazione assistita vi guiderà nelle operazioni successive.
Una volta create o importate le nostre chiavi, sempre nelle impostazioni del proprio account dentro alla sezione "Crittografia End-to-End", selezioniamo la chiave che vogliamo usare. Lasciamo tutte le altre impostazioni come sono configurate di default, e in particolare non scegliamo di attivare la crittografia per impostazione predefinita, a meno di non volere che per l'invio di qualsiasi nostra mail venga richiesto l'uso della crittografia. Preferendo l'opzione "Non attivare la crittografia per impostazione predefinita", saremo noi a decidere quando vogliamo cifrare o no una mail.
Possiamo trovare ulteriori informazioni direttamente sul sito di Thunderbird: tosegi.vado.li.

8 Cap. 19

# 19 | Usare OpenPGP

Lo standard internet[1] OpenPGP è un formato di crittografia che consente nello specifico di creare[2] e verificare[3] firme digitali, nonché di cifrare[4] e decifrare[5] email o file.
Qui andremo a dettagliare i diversi strumenti crittografici che hanno in comune l'uso di OpenPGP.

## 19.1 Importare una chiave OpenPGP

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: pochi minuti.

Lo scopo di questo capitolo è imparare a importare una chiave OpenPGP, che useremo per verificare delle firme digitali o cifrare dei messaggi. La procedura è la stessa sotto Tails o con una Debian cifrata.
Apriamo "Password e chiavi" premendo il tasto ⊞ (⌘su Mac) per aprire la panoramica delle "Attività", quindi digitiamo `pass` e infine facciamo clic sul software corrispondente.
Nella colonna di sinistra, clicchiamo su "Chiavi PGP"→ "Chiavi GnuPG".
Importare una chiave non significa aver verificato che appar-

1 Wikipedia, *Standard Internet.*
2 Cap. 19.10
3 Cap. 19.8
4 Cap. 19.6
5 Cap. 19.7

tenga al presunto proprietario. Vedremo nel prossimo capitolo che per fare questo bisogna effettuare altre operazioni, come controllare le sue firme o la sua impronta digitale.

### 19.1.1 Visualizzare le chiavi disponibili

Per visualizzare le chiavi importate, clicchiamo su Visualizza. Scegliamo “Per portachiavi” e “Mostra qualsiasi”.

### 19.1.2 Se disponiamo di una chiave su file

Clicchiamo su “File” → “Importa...” nella finestra che si aprirà, selezioniamo il file contenente la chiave, poi facciamo clic su “Apri”. Una finestra mostrerà le informazioni sulla chiave. Se questa è la chiave che si desideriamo importare, clicchiamo su “Importa”.

### 19.1.3 Se si vuole cercare la chiave online

Sempre nella finestra “Password e chiavi”, clicchiamo su “Remoto” → “Cerca chiavi remote...”
Nella finestra che si apre, digitiamo un nome, un numero di chiave o qualsiasi altra informazione che permetta di trovare la chiave cercata, per esempio: “”0x63FEE659””, “”63FEE659”” o “”Alice Dupont””. Quindi clicchiamo su “Cerca”.
Si aprirà una finestra di risultati. Potrebbero esserci anche molti nomi che corrispondono alla nostra ricerca. Quale scegliere? Se sappiamo che la chiave che stiamo cercando ha l’identificatore 63FEE659, facciamo clic con il pulsante destro del mouse su uno dei risultati e andiamo su “Proprietà”. Si

potrà così confrontare l'impronta digitale della chiave selezionata con quella desiderata. Una volta trovata la chiave corretta, selezioniamola e facciamo clic su "Importa", poi possiamo chiudere la finestra.
Tuttavia, l'id di una chiave, per esempio 63FEE659, non è sufficiente per selezionare in modo univoco una chiave[6].
La chiave importata dovrebbe ora essere visibile nel portachiavi PGP.

## 19.2 Verificare l'autenticità di una chiave pubblica

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da qualche minuto a mezz'ora.

Quando si utilizza la crittografia asimmetrica, è fondamentale assicurarsi di disporre della vera chiave pubblica del nostro corrispondente[7]. Altrimenti ci stiamo esponendo a un attacco Man in the Middle[8]: stiamo sì autenticando o cifrando la nostra corrispondenza... ma per il nostro avversario.
Dovremo prima di tutto scegliere un metodo per assicurarci di disporre della giusta chiave pubblica. Diremo quindi a OpenPGP che ci fidiamo di questa chiave.

---

6 Riseup, *Bonnes pratiques pour l'utilisation d'OpenPGP* [coparu.vado.li].
7 Cap. 6.4
8 Cap. 6.4.1

### 19.2.1 Una questione di fiducia

A seconda delle esigenze del nostro modello di rischio[9] e delle nostre possibilità, possiamo scegliere diversi modi per verificare l'autenticità di una chiave pubblica. Ipotizziamo di dovere verificare l'autenticità della chiave pubblica di Alice.

**Trasmettersi la chiave su un canale sicuro**
Quando è possibile, il modo più semplice è passarsi a mano, utilizzando ad esempio una penna USB, il file contenente la chiave pubblica. Alice esporta la sua chiave pubblica in un file[10], che memorizza su una penna USB, eventualmente cifrata[11], che poi ci fornisce. A questo punto importeremo direttamente la chiave pubblica di Alice da questo file.

**Trasmettersi il fingerprint su un canale sicuro**
Uno degli svantaggi del metodo precedente è che richiede di passarsi un file attraverso un mezzo sicuro. Questo non sempre è possibile. Fortunatamente però, questo non è nemmeno sempre necessario: generalmente è sufficiente ottenere, in modo sicuro, il checksum[12] della chiave pubblica, quello che viene chiamato "fingerprint".
Alice può quindi pubblicare la sua chiave pubblica su internet, ad esempio sul suo blog o su un keyserver. Da parte nostra, scarichiamo questa chiave in un file non autenticato, quindi controlliamo che il fingerprint della chiave corrisponda a quella che Alice ci ha fatto pervenire in modo autenticato. Per vedere il fingerprint della chiave di Alice scaricata da internet, dovremo importarla[13] nel nostro portachiavi e poi accedere

---

9 Tomo I, cap. 7
10 Cap. 19.5
11 Tomo I, cap. 18
12 Tomo I, cap. 5.2
13 Cap. 19.1

alla scheda "Dettagli" disponibile facendo doppio clic sulla sua chiave.
Cosa ci guadagniamo a usare questo metodo? Che, invece di doversi scambiare un intero file, è sufficiente trasmettere una riga di caratteri come questa:

```
A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

Ad esempio, Alice, che è una persona ben organizzata, potrebbe aver fatto una copia del fingerprint della sua chiave pubblica scritta su un pezzo di carta. In questo modo è sufficiente solo incrociarla per strada perché ce la passi: non c'è bisogno di un computer né di una penna USB.
Se non possiamo incontrare Alice, potrà inviarci il fingerprint anche per posta ordinaria, oppure potremo chiamarla perché ce la legga per telefono. La verifica sarà meno sicura che vedendosi direttamente, ma è piuttosto difficile che un avversario ci invii una lettera postale con la sua chiave o risponda al numero di telefono di Alice leggendoci il suo fingerprint, imitando la sua voce.
Questo diventa più complicato se non si conosce Alice. In questo caso, dovremo acquisire confidenza con delle persone che affermano di conoscerla. Ancora una volta, non esistono formule magiche, ma la combinazione di diversi mezzi di verifica complica il compito di un possibile avversario che desideri lanciare un attacco Man in the Middle[14]: possiamo chiedere a più persone che sostengono di conoscere Alice piuttosto che a una sola, utilizzare mezzi di comunicazione diversi, ecc.

**Utilizzare il Web of Trust**
OpenPGP integra la nozione di *fiducia transitiva* con il Web of Trust[15]. Una volta che la chiave di Alice è stata scaricata,

14 Cap. 6.4.1
15 Cap. 6.4.3

possiamo elencare le identità che hanno firmato la sua chiave: queste persone dichiarano pubblicamente di aver verificato che questa chiave appartenga effettivamente ad Alice. Se conosciamo una di queste persone o una terza parte che si fida di una di queste persone, OpenPGP può creare percorsi di fiducia tra le identità di cui ci si fida e le altre con cui desideriamo comunicare.

## 19.3 Firmare una chiave

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Una volta che abbiamo verificato l'attendibilità della chiave di Alice, è utile informare OpenPGP che può fidarsi della sua chiave. Questa operazione si chiama "Firmare" una chiave. La procedura è la stessa in Tails o con una Debian cifrata.
Abbiamo due opzioni:

- firmare la chiave di Alice localmente, il che ci permette di non rivelare che la nostra identità è *collegata* a quella di Alice;
- firmare pubblicamente la chiave di Alice, consentendo a qualsiasi utente del Web of Trust di approfittare delle verifiche che abbiamo fatto.

Ancora una volta, nessuna buona risposta, ma una scelta da fare in base alle nostre esigenze e alla nostra policy di sicurezza.
Apriamo "Password e chiavi" premendo il tasto ⊞ (⌘ su Mac) per aprire la panoramica delle "Attività", quindi digitiamo `pass` e infine facciamo clic sul software corrispondente.

Per vedere le chiavi OpenPGP, clicchiamo sul menu “Visualizza” → “Mostra qualsiasi” e selezioniamo la casella “Per portachiavi” nello stesso menu.
Se la chiave non è presente, importiamola[16].
Una volta che la chiave di Alice si trova nella finestra principale, facciamo doppio clic su di essa per visualizzare i dettagli della chiave. Verifichiamo che sia la chiave giusta, ad esempio controllando il suo fingerprint nella scheda “Proprietà”. Quindi scegliamo la scheda “Fiducia” e clicchiamo su “Firma questa chiave”.
Scegliamo quanto attentamente abbiamo controllato la chiave, ad esempio “Superficialmente” se abbiamo verificato il fingerprint a telefono, o “Molto attentamente” se conosciamo bene Alice e ci ha dato la sua chiave o il suo fingerprint di mano propria.
Nella parte inferiore della finestra, clicchiamo su “Non consentire agli altri di vedere questa firma” se desideriamo nascondere i collegamenti tra la nostra identità e Alice.
Quindi facciamo clic su “Firma”, e inseriamo la passphrase della nostra chiave privata nella casella finestra di dialogo che apparirà.
Potrebbe apparire la finestra “Impossibile firmare la chiave”, in tal caso facciamo clic su “Chiudi” e ripetiamo l’operazione di firma dal passaggio precedente.
OpenPGP ora sa che la chiave di Alice è attendibile.
Se vogliamo aggiungere questa chiave al nostro Web of Trust[17], dopo averla firmata possiamo pubblicarla sui keyserver pubblici[18].

16 Cap. 19.1
17 Cap. 6.4.3
18 Cap. 19.5

## 19.4 Creare e mantenere una coppia di chiavi

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 15 minuti a un'ora.

In questo capitolo tratteremo la creazione e parte della gestione di una coppia di chiavi di cifratura. È bene tenere bene a mente alcune nozioni di base. Anzitutto, il fatto che non tutte le chiavi di cifratura utilizzano lo stesso algoritmo. Abbiamo parlato della crittografia RSA[19] ma ce ne sono molte altre. E comunque se le chiavi di cifratura utilizzano effettivamente lo stesso algoritmo, non hanno necessariamente la stessa dimensione. Inoltre, alcuni hanno una data di scadenza, altri no.

### 19.4.1 Creare una coppia di chiavi

Per creare una coppia di chiavi, avviamo "Password e chiavi" premendo il tasto ⊞ (⌘su Mac), quindi digitando `pass` e infine facendo clic sul software corrispondente.
Nella finestra che si aprirà, clicchiamo sul pulsante "Nuovo..." nel menu "File". Selezioniamo quindi "Chiave PGP" e clicchiamo su "Continua".
Si aprirà una nuova finestra. Immettiamo un *Nome completo* corrispondente all'identità contestuale[20] utilizzata, nonché l'indirizzo email ad essa associato. È possibile inserire l'identificativo dell'indirizzo email prima del simbolo @ come *Nome completo*, ma deve essere lungo almeno 5 caratteri. Dentro

19 Cap. 6.2.1
20 Cap. 5.1

"Opzioni avanzate" scegliamo la dimensione della chiave e la data di scadenza. Il "Tipo di cifratura" predefinito è RSA. Lasciamolo così com'è. La "Dimensione della chiave" proposta di default, 2048 bit, è considerata sicura fino al 2030[21]. È possibile scegliere la dimensione della chiave più alta disponibile, vale a dire 4096 bit, se si desidera proteggere le comunicazioni in modo più forte o più a lungo. È consigliabile scegliere una "Data di scadenza" per la chiave. Se è la prima volta che creiamo una coppia di chiavi, sceglieremo una data di scadenza compresa ad esempio tra 1 e 2 anni. Per non dimenticare di rinnovare la chiave in tempo, potrebbe essere una buona idea annotarsi da qualche parte questa data di scadenza.
Infine facciamo clic su "Crea".
Si aprirà una nuova finestra, che ci domanderà una passphrase per proteggere la chiave. Ora è il momento di scegliere una buona passphrase e digitarla due volte, prima di fare clic su "Convalida". Attenzione tuttavia a non confondere la passphrase fornita qui con una delle chiavi della coppia di chiavi di cifratura. La passphrase serve unicamente a limitare l'uso della chiave privata della nostra coppia.
Questa operazione può essere quasi istantanea o richiedere diversi minuti. Ora è il momento di spostare il mouse, utilizzare la tastiera o anche utilizzare il disco rigido, se possibile, per aiutare il computer a generare dati casuali. Questi sono necessari per il processo di generazione delle chiavi.
Terminata questa operazione, la nostra chiave apparirà nel software "Password e chiavi". Può capitare che la chiave non sia visibile; in questo caso, spostiamoci in alto o in basso nell'elenco delle chiavi[22].

---

21 Agence nationale de la sécurité des systèmes d'information, 2014, *Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [tularo.vado.li].
22 Zvi Gutterman, Benny Pinkas, Tzachy Reinman, *Analysis of the Linux Random Number Generator* [nopimi.vado.li].

Effettuato questo passaggio di creazione delle chiavi, è bene pensare a come salvaguardare la nostra coppia di chiavi. Essendo in parte segrete, si tratta di non lasciarle uscire da nessuna parte. La chiave privata deve essere accessibile unicamente alla persona che dovrebbe avervi accesso. La cosa migliore è mantenere questa coppia di chiavi su un volume cifrato[23], che si tratti di una penna USB, di un disco rigido interno o esterno o della persistenza di Tails[24].

### 19.4.2 Esportare la tua chiave pubblica

Affinché si possano ricevere email cifrate, chi ce le invia deve disporre della nostra chiave pubblica. Per fare ciò, la chiave dovrà essere esportata dal software "Password e chiavi" per inviarla ai nostri corrispondenti.
Vedremo più avanti come esportare una chiave[25].

### 19.4.3 Pubblicare una chiave pubblica sui keyserver

Se l'esistenza dell'identità contestuale[26] a cui corrisponde la chiave non è di per sé riservata, possiamo pubblicare la nostra chiave pubblica su un keyserver, in modo che chiunque desideri inviarci email cifrate possa scaricarla a questo scopo. Per fare ciò, clicchiamo sulla sua chiave e poi su "Sincronizza e pubblica le chiavi..." dentro il menu "Remoto". Verrà visualizzata una finestra "Sincronizza chiavi".
Se viene visualizzato un messaggio, dato che nessun keyserver è stato selezionato per la pubblicazione, le proprie chiavi non

---

23 Tomo I, cap. 18
24 Tomo I, cap. 14.5
25 Cap. 19.5
26 Cap. 5

saranno rese disponibili ad altri.
Facciamo clic su “Server di chiavi” e scegliamo un server nel menu a tendina in corrispondenza di “Pubblicare le chiavi in:”, quindi clicchiamo su “Chiudi”.
Clicchiamo adesso su “Sincronizza” per pubblicare la chiave.

### 19.4.4 Ottenere il fingerprint di una chiave

Se trasmettiamo la nostra chiave pubblica con un mezzo non autenticato (ad esempio una email non firmata), può essere utile far pervenire al nostro corrispondente il fingerprint[27] della nostra chiave con un mezzo autenticato, in modo che possa assicurarsi della sua integrità. Il fingerprint è accessibile nella scheda “Dettagli” disponibile facendo doppio clic su una chiave. Potremmo ad esempio scriverla su un pezzo di carta che consegneremo al nostro corrispondente.

### 19.4.5 Generare un certificato di revoca e tenerlo al sicuro

Se un avversario si impossessa della nostra chiave privata, o se semplicemente la perdiamo, è necessario revocarla, così che i nostri corrispondenti sappiano che non deve più essere utilizzata. Per questo, si crea un certificato di revoca.
È consigliato creare il certificato di revoca subito dopo aver generato la coppia di chiavi, perché se perdiamo la chiave o dimentichiamo la nostra passphrase, non saremo più in grado di creare un certificato di revoca.
Il certificato di revoca si presenta sotto forma di file o di qualche riga di “testo”, che dovremo conservare in un luogo sicuro,

27 Tomo I, cap. 5.2.2

ad esempio su una penna USB cifrata, presso una persona fidata o su un foglio ben nascosto. Infatti, chiunque abbia accesso a questo file può revocare la nostra coppia di chiavi e quindi impedirci di comunicare.
Per generare il certificato, purtroppo, si deve usare un Terminale[28].
Inizieremo digitando il comando (senza premere Invio):

```
gpg –gen-revoke
```

Digitiamo quindi l'identificatore della nostra chiave, accessibile nella scheda "Proprietario", disponibile facendo doppio clic sulla chiave.
Questo dovrebbe darci qualcosa come:

```
gpg –gen-revoke 2A544427
```

Premiamo quindi il tasto "Invio" per eseguire il comando.
GnuPG poi ci porrà alcune domande in inglese:

```
sec  rsa2048/2A544427162BCC15 2013-09-24 Alice (esempio)
<alice@example.org>
Create a revocation certificate for this key? (y/N)
```

Poiché ci viene chiesto se vogliamo creare un certificato di revoca per la nostra chiave, digitiamo `y` e premiamo "Invio". Il Terminale ci restituirà:

```
sec  rsa2048/2A544427162BCC15 2013-09-24 Alice (esempio)
<alice@example.org>
Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
```

28 Tomo I, cap. 11

```
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision?
```

Stiamo preparando un certificato nel caso in cui la nostra chiave venga compromessa. Digiteremo quindi il numero `1`, e premeremo il tasto “Invio”.
GnuPG ci chiede adesso una descrizione del problema:

```
Enter an optional description; end it with an empty line:
```

Non lo sappiamo, poiché la chiave non è ancora compromessa, e quindi lasceremo semplicemente vuoto il campo della descrizione premendo di nuovo Invio.
GnuPG ci chiede conferma:

```
Reason for revocation: Key has been compromised
(No description given)
Is this okay ? (y/N)
```

Premiamo `y` e poi il tasto “Invio” per accettare. GnuPG ci chiederà allora la passphrase associata a questa coppia di chiavi, quindi visualizzerà il certificato di revoca:

```
ASCII armored output forced.
-–BEGIN PGP PUBLIC KEY BLOCK—–-
Comment: This is a revocation certificate
iQEfBCABCgAJBQJSQZVMAh0CAAoJEM YS/iAqVEQnzFsH/3NM-
zeXy0XbOJ3Q+g2mAxEAl4G8VesEYDE8LHzemNmkyrrMKNGpllPJ-
VkyMXKBLYTojQjjL6QhL1nyqaUavseOmaa1Swa9PgI6AJZrk-
```

miMk74CCXJq QDb5uupZNQ3UsoGHqKcirYUHyOeEQ/m94QxMaPjpC-
Mi9tIJjnb1T8svDuwhpsh2G jZhOuyUedyyD4r/noT8YYhWKNC98El-
PQkHVVEzu6TJu0IKRp7OJgPCb8cJ6odsm3 jPxjIF+f/cz9WIu-
d8EB3HJVIxoMm183XI+HtddcOxSsdIljuk6ddqgyQDTPJVex+EY-
dG0FreT7OrFzKXo316/4RSWKX/klshSp
O/8=
=cpvr
---END PGP PUBLIC KEY BLOCK—-

```
Revocation certificate created.
Please move it to a medium which you can hide away; if Mallory gets access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case your media become unreadable. But have some caution: The print system of your machine might store the data and make it available to others!
```

Il certificato è la parte che va dalla riga che contiene `BEGIN PGP PUBLIC KEY BLOCK` fino a quella che contiene `END PGP PUBLIC KEY BLOCK`. Per salvarlo, inizieremo selezionandolo e copiandolo negli appunti (tasto destro e poi "Copia"), quindi apriremo l'Editor di testo "gedit" (accessibile premendo il tasto ⊞ (⌘su Mac), digitando `testo` e facendo quindi clic su "gedit"), dopodiché lo incolleremo in un nuovo documento (clic col destro e poi "Incolla").
A seconda della nostra scelta, potremo quindi:

- salvarlo facendo clic su "Salva". È importante scegliere un nome chiaro per il file, ad esempio C`ertificato di revoca per chiave 2A544427`;
- stamparlo cliccando su "Stampa", dal menu ☰.

Se la nostra chiave dovesse essere compromessa, useremmo questo certificato per revocarla[29].

29 Cap. 19.11

### 19.4.6 Effettuare la transizione verso una nuova coppia di chiavi

Prima che la nostra coppia di chiavi scada, o quando i progressi della crittografia ci costringeranno a usare chiavi più sicure, dovremo creare una nuova coppia di chiavi. Per fare questo seguiremo le istruzioni qui sopra.
Sarà poi nostra cura firmare la nostra nuova chiave con la vecchia seguendo la sezione "Firmare una chiave" dello strumento per verificare l'autenticità di una chiave[30]. Quindi esporteremo la nostra nuova chiave e la faremo pervenire alle persone con le quali comunichiamo.
Qualche mese dopo, potremo revocare[31] la nostra vecchia chiave.

### 19.4.7 Estendere la coppia di chiavi

Nel caso in cui la nostra coppia di chiavi scada, ma non ci sia motivo di passare a una nuova coppia, possiamo sempre prolungarne la validità. Per fare ciò, in "Password e chiavi", facciamo doppio clic sulla nostra coppia di chiavi, quindi andiamo alla scheda "Proprietà" e poi "Dettagli". Nella parte "Sottochiavi", vediamo che ci sono due righe che corrispondono alla nostra chiave di cifratura e di firma. Dovremo modificare la data di scadenza di entrambe. Per fare ciò, selezioniamo una delle due sottochiavi cliccandoci sopra e poi cliccando sul pulsante "Scade". Selezioniamo una nuova data di scadenza e poi clicchiamo su "Modifica". Ci viene richiesta la passphrase associata alla nostra coppia di chiavi; inseriamola e clicchiamo su "OK". Constatiamo che la data nella colonna "Scadenza" è cambiata. Ripetiamo la stessa operazione per l'altra sotto-

30 Cap. 19.3
31 Cap. 19.11

chiave della coppia.
Ed eccoci di nuovo pronti per un'altra stagione con la nostra coppia di chiavi!

## 19.5 Esportare una chiave pubblica OpenPGP

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Lo scopo di questa ricetta è esportare una chiave OpenPGP, che utilizzeremo ad esempio per trasmetterla ai nostri contatti in modo che possano scriverci, o per verificare le firme digitali. La procedura è la stessa sotto Tails o con una Debian cifrata.
Apriamo "Password e chiavi" premendo il tasto ⊞ (⌘su Mac), quindi digitiamo `pass` e infine clicchiamo sul software corrispondente.

### 19.5.1 Mostrare le chiavi disponibili

Per visualizzare le chiavi importate, fare clic su "Visualizza" → "Mostra qualsiasi". Scegliere "Per portachiavi".

### 19.5.2 Per esportare la chiave in un file

Il file che andremo ad esportare conterrà la nostra chiave pubblica, necessaria per chi voglia inviarci email cifrate. An-

diamo su “Password e chiavi”, selezioniamo la nostra chiave OpenPGP e scegliamo “Esporta...” nel menu “File”. In basso a destra, nella finestra che si aprirà, scegliamo “Chiavi PGP con armatura” dal menu a a tendina invece di “Chiavi PGP”. Scegliamo un percorso di esportazione e un nome file, quindi facciamo clic su “Esporta”.

### 19.5.3 Per esportare la chiave su un keyserver

Abbiamo già visto come pubblicare la nostra chiave pubblica sui keyserver[32].

## 19.6 Utilizzare la crittografia asimmetrica per cifrare le proprie email

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Adesso esploreremo l’uso della crittografia asimmetrica nel caso specifico della cifratura della posta elettronica.
A seconda che si stia utilizzando un client di posta o una webmail, il metodo da utilizzare per cifrare le nostre email sarà diverso.
Tuttavia va notato che l’oggetto di un’email cifrata non è cifrato. Potremmo anche evitare di inserirvi informazioni che consideriamo sensibili.

32 Cap. 19.4

### 19.6.1 Cifrare le proprie email con Thunderbird

Per questa procedura vi rimandiamo al capitolo su Thunderbird[33].

### 19.6.2 Cifrare le proprie email con una webmail dentro Tails

Se preferiamo cifrare le nostre email utilizzando una webmail, evitiamo di digitare il nostro messaggio nella finestra del browser web per poi cifrarlo in seguito. In effetti certi attacchi, in particolare quelli tramite JavaScript[34], possono arrivare al nostro testo da questo stesso browser. Inoltre, il testo scritto all'interno della webmail potrebbe venire salvato in automatico, non cifrato, nelle bozze. Sarebbe molto spiacevole offrire in chiaro[35] un testo che si desiderava invece cifrare.
Qui di seguito spiegheremo unicamente come cifrare le nostre mail tramite webmail con Tails[36].
Il metodo attualmente consigliato per cifrare un'email, nonché per cifrare il testo, è descritto nella documentazione di Tails.
Una volta avviato Tails[37], visualizziamo il Desktop e facciamo clic sull'icona "Documentazione di Tails". Nel menu a destra, clicchiamo su "Documentazione".
Nell'indice che si apre, cerchiamo la sezione "Cifratura e privacy" e facciamo clic sulla pagina "Encrypting and signing text using public-key cryptography". Seguiamo dunque questa pagina di documentazione.

33 Cap. 18
34 Cap. 2.1.3
35 Tomo I, cap. 5.1.1
36 Tomo I, cap. 14.4
37 Tomo I, cap. 14.4

## 19.7 Decifrare le email

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Dopo aver scelto un metodo per gestire la propria posta elettronica[38], dopo aver visto come creare e mantenere una coppia di chiavi[39] e come cifrare le email[40], vediamo adesso come decifrarle.
Anche in questo caso esistono diversi metodi a seconda degli strumenti utilizzati.

### 19.7.1 Decifrare le proprie email con Thunderbird

Per questa procedura vi rimandiamo al capitolo su Thunderbird[41].

### 19.7.2 Decifrare le proprie email con una webmail dentro Tails

Ecco come decifrare le email per una webmail con Tails.
Come per cifrare un'email, è necessario evitare di decifrarla direttamente nella finestra della webmail. Alcuni attacchi Ja-

38 Cap. 10.4
39 Cap. 19.4
40 Cap. 19.6.2
41 Cap. 18

vaScript[42] hanno possibilità di arrivare al testo attraverso il browser web che stiamo utilizzando.
Una volta avviato Tails[43], visualizzamo il Desktop e clicchiamo sull'icona "Documentazione di Tails". Nel menu a destra, clicchiamo su "Documentazione". Nell'indice che si apre, cerchiamo la sezione "Crittografia e privacy" e facciamo clic sulla pagina "Decrypting and verify text". Seguiamo questa pagina di documentazione.

## 19.8 Verificare una firma OpenPGP

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Lo scopo di questa ricetta è verificare l'autenticità di un file con una firma OpenPGP[44]. Gli autori di questa guida non hanno finora trovato uno strumento grafico per un serio controllo delle firme che sia incluso sia in Tails che nell'attuale versione di Debian. Apriamo quindi un Terminale[45] per fare queste verifiche. Iniziamo digitando il comando (*senza* dare "Invio"):

```
gpg -- verify
```

Dopo aggiungiamo uno spazio, quindi clicchiamo sull'icona del file della firma (spesso con suffisso `.sig` o `.asc`) e trascinia-

42 Cap.2.1.3
43 Tomo I, cap. 14.2.3
44 Cap. 6.3
45 Tomo I, cap.11

molo nel Terminale. Dopo aver rilasciato il tasto, ciò che verrà visualizzato dovrebbe somigliare a:

```
gpg –verify '/home/amnesia/tails-i386-2.7.iso.sig'
```

Quindi prendiamo l'icona del file da controllare e trasciniamo anch'esso nel terminale. Dopo averlo rilasciato, ciò che verrà visualizzato dovrebbe essere simile a:

```
gpg –verify '/home/amnesia/tails-i386-2.7.iso.sig' '/
home/amnesia/tails-i386-2.7.iso'
```

Premiamo quindi il tasto "Invio" per avviare il controllo. Potrebbero essere necessari diversi minuti a seconda delle dimensioni del file e della potenza del computer che si utilizza. Quando il controllo è completo, si dovrebbe visualizzare qualcosa che assomiglia a:

```
gpg: Firma eseguita lun 12 lug 2021, 14:56:35 CEST
gpg: con RSA chiave 05469FB85EAD6589B43D41D3D21DA-
D38AF281C0B
gpg: Firma valida per « Tails developers (offline long-term
identity key) < tails@boum.org > »
```

Queste poche righe potrebbero essere seguite da qualcosa come:

```
gpg: Attenzione: questa chiave non è validata attraverso
una firma di fiducia.
gpg: Niente ci dice che la firma appartenga al suo proprie-
tario.
Checksum della chiave principale: A490 D0F4 D311 A415 3E2B
B7CA DBB8 02B2 58AC D84F
```

```
Checksum della sottochiave: 7919 2EE2 2044 9071 F589 AC00
AF29 2B44 A0ED AA41
```

Queste righe non ci indicano che la firma non è valida, ma soltanto che non è stata ancora verificata l'autenticità[46] della chiave pubblica della persona che firma i dati, e che un avversario potrebbe eseguire un attacco Man in the Middle[47].
Se la firma non è corretta, il computer visualizzerà qualcosa del tipo:

```
gpg: Firma eseguita lun 12 lug 2021, 14:56:35 CEST
gpg: con RSA chiave RSA 0×98FEC6BC752A3DB6
gpg: Firma errata per « Tails developers (offline long-term
identity key) < tails@boum.org > »
```

## 19.9 Firmare le email

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Come spiegato nella sezione sulle firme digitali[48], potremmo volerci assicurare dell'autenticità[49] di un messaggio. Ora vedremo come firmare digitalmente le email per fornire almeno una garanzia della loro integrità e, nel migliore dei casi, una garanzia della loro autenticità.

46 Cap. 19.2
47 Cap. 6.4.1
48 Cap. 6.3
49 Tomo I, cap. 5

**Da Thunderbird**
Una volta avviato e configurato Thunderbird[50], facciamo clic sul pulsante “Scrivi” per iniziare a scrivere un nuovo messaggio. Si aprirà una finestra di scrittura in cui scriveremo la nostra email. Prima o dopo aver scritto l’email, ma comunque prima di inviarla, clicchiamo sul menu “Sicurezza”, poi spuntiamo l’opzione “Apponi firma digitale”.
Una volta completata la nostra email, facciamo clic su “Invia”. Si aprirà la finestra che ci chiederà di inserire la passphrase associata alla coppia di chiavi che verrà utilizzata per firmare il messaggio.

**Da una webmail**
Non ci sono strumenti che possiamo consigliare per firmare email per una webmail con una Debian cifrata. Per firmare le nostre email utilizzando una webmail in Tails, possiamo invece seguire la procedura seguente.
Il metodo attualmente consigliato per firmare un’email, oltre che un testo, è descritto nella documentazione di Tails.
Una volta avviato Tails[51], visualizziamo il Desktop e clicchiamo sull’icona “Documentazione di Tails”. Nel menu a destra, facciamo clic su “Documentazione”. Nell’indice che si aprirà, cerchiamo la sezione “Crittografia e privacy” e clicchiamo sulla pagina “Encrypting and signing text using public-key cryptography”. Seguiamo dunque questa pagina di documentazione.

## 19.10 Firmare dei dati

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che tro-

50 Cap. 18
51 Tomo I, cap. 14.4

verete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

Lo scopo di questa ricetta è apporre una firma digitale[52] ai dati. Ciò può servire per autenticare l'autore di un messaggio o di un file, verificare il software, ecc. Questa ricetta richiede di aver precedentemente generato una coppia di chiavi[53].

### 19.10.1 Firmare il testo con Tails

Una volta avviato Tails[54], visualizziamo il Desktop e facciamo clic sull'icona "Documentazione di Tails". Nel menu a destra, facciamo clic su "Documentazione". Nell'indice che si aprirà, cerchiamo la sezione "Crittografia e privacy", clicchiamo sulla pagina "Encrypting and signing text using public-key cryptography" e seguiamo la pagina di documentazione.

### 19.10.2 Firmare un file

Se stiamo utilizzando una Debian cifrata[55], dobbiamo prima installare[56] il pacchetto `seahorse-nautilus`. Se usiamo Tails, il pacchetto per la firma dei file richiesto è già installato.
Per firmare un file, facciamo clic col tasto destro del mouse su di esso e selezioniamo "Firma nel menu contestuale". Verrà visualizzata la finestra "Scegli il firmatario". Davanti al menu

52 Cap. 6.3
53 Cap. 19.4
54 Tomo I, cap. 14.4
55 Tomo I, cap. 15
56 Tomo I, cap. 16.3

a tendina “Firma il messaggio come:”, scegliamo l’identità contestuale desiderata, quindi clicchiamo su “Convalida”. Si aprirà una finestra in cui è necessario digitare la passphrase corrispondente alla chiave privata dell’identità scelta, quindi facciamo clic su “OK”.
Il processo di firma può richiedere fino a diversi minuti a seconda delle dimensioni del file e della potenza del computer che si utilizza. Una volta completata la firma, essa si presenterà sotto forma di un piccolo file con lo stesso nome del file originale, ma che termina con l’estensione `.sig`, che si trova nella stessa posizione del file originale e che dovremo trasmettere al nostro interlocutore assieme a esso.

## 19.11 Revocare una coppia di chiavi

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 15 a 30 minuti.

Se la nostra chiave privata fosse compromessa, dovremmo far pervenire il certificato di revoca creato in precedenza[57] ai nostri corrispondenti, in modo che non possano più utilizzarla e sappiano che non è più attendibile.

*Attenzione*: le istruzioni che seguono revocheranno irreversibilmente la nostra chiave. Vanno usate con moderazione!

57 Cap. 19.4

### 19.11.1 Fare sapere che la nostra coppia di chiavi è compromessa

Nel caso in cui la nostra coppia di chiavi sia compromessa, ad esempio se è stata ottenuta dopo un'intrusione nel nostro sistema, l'obiettivo è quello di farlo sapere ai nostri corrispondenti. Sia con Tails che con una Debian cifrata, dovremo prima di tutto importare questo certificato di revoca.

**Importare il certificato di revoca**
Se si utilizza una Debian cifrata[58], servirà innanzitutto installare[59] il pacchetto `seahorse-nautilus`. Se si utilizza Tails, il pacchetto necessario per l'importazione del certificato di revoca è già installato.
Per importare il certificato, facciamo clic destro su di esso e selezioniamo "Apri e Importa una chiave" dal menu di scelta contestuale.
Al momento della scrittura di questa guida, è ancora presente il messaggio di errore "Importazione non riuscita. Le chiavi sono state trovate, ma non importate." che si apre dopo aver eseguito l'ultima operazione. Ma questo non dovrebbe alterare la revoca desiderata.
Inoltre, per verificare l'effettiva revoca della chiave, è necessario avviare "Password e chiavi" dalla panoramica "Attività" premendo il tasto ⊞ (⌘ su Mac) quindi digitando `pass` e facendo clic sul software corrispondente. Nella lista delle chiavi, il nome delle chiavi revocate è barrato, quindi dovremo controllare che quella revocata in precedenza sia effettivamente barrata.
Dobbiamo ancora far sapere ai nostri corrispondenti che la nostra coppia di chiavi è stata compromessa, perché per il momento solo il nostro computer ne è a conoscenza. Per rimedia-

58 Tomo I, cap. 15
59 Tomo I, cap. 16.3

re a questo possiamo pubblicare la nostra chiave ora revocata. Dovremo quindi dire ai nostri corrispondenti, ad esempio via email, che devono sincronizzarsi con il keyserver[60] per revocare la nostra chiave pubblica in loro possesso. Se invece non abbiamo pubblicato la nostra chiave pubblica su un keyserver, dovremo includere il certificato di revoca in una email inviata ai nostri corrispondenti.

**Pubblicare la coppia di chiavi revocata**

Se la nostra chiave pubblica è stata precedentemente pubblicata su un keyserver[61], la cosa migliore è sincronizzarsi con questo stesso server, in modo che la nostra chiave pubblica venga revocata anche lì, consentendo così a tutti i nostri corrispondenti di essere avvisati. Però attenzione: se non viene selezionata alcuna chiave, l'intero portachiavi verrà inviato al server delle chiavi.

Tuttavia, se viene selezionata una singola chiave e viene comunque proposto di inviare l'intero portachiavi al keyserver, bisognerà cliccare su "Annulla" e chiudere la finestra "Password e chiavi". Poi sarà necessario seguire i passaggi del paragrafo precedente "Pubblicare la coppia di chiavi revocata".

Per fare ciò, sia sotto Tails che in una Debian, avviamo "Password e chiavi" dalla panoramica delle attività premendo il tasto ⊞ (⌘su Mac) e digitando `pass`. Quindi seguiamo la parte "Pubblicare la chiave pubblica sui server delle chiavi" per creare e mantenere una coppia di chiavi[62].

Una volta effettuata questa sincronizzazione, resta da informare i nostri corrispondenti. Non esiste una ricetta già pronta per questo, tra inviare loro un'email cifrata, farglielo sapere di persona, ecc.

---

60 Cap. 19.4

61 Cap. 19.4

62 Cap. 19.4

### 19.11.2 Revocare la coppia di chiavi di un corrispondente

Se uno dei nostri corrispondenti ci ha fatto sapere che la sua coppia di chiavi è compromessa e che l'ha revocata, dobbiamo aggiornarla sul nostro computer, sia che ci si trovi sotto Tails sia in una Debian cifrata.

**Sincronizzarsi con un keyserver**
Nel caso in cui il nostro corrispondente abbia aggiornato su un keyserver la sua chiave pubblica, che è stata ormai revocata, dovremo semplicemente sincronizzarci con questo keyserver. Per farlo, avviamo "Password e chiavi" dalla panoramica delle attività premendo il tasto ⊞ (⌘su Mac) e digitando `pass`. Selezioniamo la chiave che vogliamo sincronizzare, facciamo clic sul menu "Remoto", quindi su "Sincronizza e pubblica chiavi..." Se non è stato scelto alcun keyserver, clicchiamo sul pulsante "Keyserver" e selezioniamo `hkp://pool.sks-keyservers.net` per Debian e `hkp://jirk5u4osbsr34t5.onion` in Tails per pubblicare le nostre chiavi. Chiudiamo la finestra e clicchiamo infine su "Sincronizza".

**Importa il certificato di revoca di un corrispondente**
Se invece la chiave compromessa del nostro corrispondente non è disponibile su un keyserver, o non è sincronizzata, e quest'ultimo ci ha inviato il certificato di revoca, dovremo importarla noi stessi. A tale scopo, seguire i passaggi nella sezione "Importare il certificato di revoca precedente" .

## 19.12 Cifrare i dati

↻ I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che tro-

verete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: qualche minuto.

L'obiettivo di questa ricetta è cifrare i dati[63]. Questo può servire in particolare per trasmettere uno o più documenti riservati su un supporto non cifrato che contiene già dati o anche per mettere online questi stessi documenti.
Se si utilizza Tails, il software necessario per la cifratura dei file è già installato. Se si utilizza una Debian cifrata[64], servirà prima di tutto installare[65] il pacchetto `seahorse-nautilus`.

### 19.12.1 Localizzare il file da cifrare

Apriamo "File", ad esempio premendo il tasto ⊞ (⌘ su Mac) per aprire la panoramica delle "Attività", quindi digitando `fil` e facendo clic sul software corrispondente.
Navighiamo per visualizzare il file che vogliamo cifrare e selezioniamolo.

### 19.12.2 Cifrare i dati con una passphrase

Facciamo clic con il pulsante destro del mouse sul file e scegliamo "Cifra..." dal menu a tendina. Se viene visualizzato un avviso in inglese che inizia con "No encryption keys were found" (Non sono state trovate chiavi di cifratura), clicchiamo su "Use a shared password" (Usa una passphrase condivisa). Altrimenti, se viene visualizzata una finestra intitolata "En-

63 Cap. 6.3
64 Tomo I, cap. 15
65 Tomo I, cap 16.3

cryption settings" (Impostazioni di crittografia), clicchiamo su "Use passphrase only", quindi clicchiamo su "Convalida". Se in precedenza abbiamo selezionato più file, una finestra ci chiederà se vogliamo "Cifrare ogni file separatamente" o "Cifrare tutto in un unico pacchetto". Scegliamo l'opzione opportuna. Se scegliamo di cifrare in un pacchetto, inseriamo il nome del pacchetto e un'estensione tra i formati di archivio proposti, quindi facciamo clic su "Convalida". Si aprirà così una finestra che chiederà di inserire la passphrase due volte. Digitiamola due volte per ogni file se sono cifrati separatamente facendo clic su "OK" ogni volta. I file cifrati verranno visualizzati a fianco dei loro originali non cifrati.

### 19.12.3 Cifrare i dati con una o più chiavi pubbliche

Prima di cominciare, è necessario avere nel proprio portachiavi le chiavi pubbliche di tutte le persone con cui si vogliono condividere questi file. Se non è già stato fatto, sarà necessario importarle[66].
A questo punto, facciamo clic con il tasto destro sui file da cifrare. Scegliamo "Cifra..." nel menu a tendina. Selezioniamo, spuntandole, le chiavi pubbliche dei destinatari dei file riservati. Non dimentichiamo di spuntare anche la nostra chiave se vogliamo che i file vengano cifrati anche per noi. Quindi clicchiamo su "Convalida". Se in precedenza abbiamo selezionato diversi file, una finestra ci chiederà se vogliamo "Cifrare ogni file separatamente" o "Cifrare tutto in un pacchetto". Scegliamo l'opzione appropriata, e il nome del pacchetto se questi file verranno crittografati insieme, quindi clicchiamo su "Convalida". I file cifrati verranno visualizzati accanto agli originali non cifrati.

---

66 Cap. 19

## 19.13 Decifrare i dati

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: pochi minuto.

L'obiettivo di questa ricetta è decifrare i file cifrati digitalmente[67]. Questo può essere utilizzato in particolare per leggere documenti riservati trasmessi in modo criptato.
Se si usa Tails, il software necessario per la cifratura dei file è già installato. Se si è sotto una Debian cifrata[68], servirà prima installare[69] il pacchetto `seahorse-nautilus`.

### 19.13.1 Individuare il file da decifrare

Apriamo "File", ad esempio premendo il tasto ⊞ (⌘ su Mac) per aprire la panoramica delle "Attività", quindi digitando `fil` e facendo clic sul software corrispondente. Navighiamo per trovare il file che desideriamo decifrare.

*Attenzione*: spostare sempre il file da decifrare nella posizione in cui si desidera salvarlo nella sua forma decrittografata. Ad esempio, se il file cifrato è archiviato su una penna USB non cifrata, sarà molto importante spostarlo prima di decifarlo, altrimenti il file decifrato finirà in chiaro sull'unità USB.

Facciamo doppio clic sul file da decifrare. Dopo aver inserito

67 Cap. 5/6.3
68 Tomo I, cap. 15
69 Tomo I, cap. 16.3

la passphrase condivisa o quella della chiave privata OpenP-GP, il file verrà decifrato e una sua copia in chiaro apparirà accanto al file cifrato.

# 20 | Utilizzare la messaggistica istantanea con OTR

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da mezz'ora a un'ora.

L'obiettivo di questo capitolo è conversare con una persona utilizzando la messaggistica istantanea con crittografia e autenticazione. Per fare ciò, utilizzeremo il protocollo OTR[1] che rende possibile aggiungere cifratura, autenticazione e Forward Secrecy[2] a una serie di protocolli di messaggistica istantanea.

## 20.1 Installare il client di messaggistica istantanea Pidgin

Per fare questo useremo il client di posta Pidgin. Effettivamente, esso ha un buon supporto per la crittografia OTR. Inoltre, consente di utilizzare diversi protocolli di messaggistica istantanea, come, tra gli altri, XMPP o IRC[3]. Questo software è installato nel sistema live Tails, ma lì sono supportati solo i protocolli XMPP e IRC, gli altri sono difficili da

1 Wikipedia, *Off-the-Record Messaging*.

2 La Forward Secrecy è una proprietà della crittografia che fa in modo di non compromettere la confidenzialità di una comunicazione che è stata intercettata anche se un avversario è entrato in possesso della chiave privata di cifratura. Cfr. Wikipedia, *Forward Secrecy*.

3 Per una lista esaustiva dei protocolli utilizzati da Pidgin, cfr. il sito web https://pidgin.im/

rendere anonimi. Su una Debian cifrata[4], bisognerà iniziare installando[5] i pacchetti pidgin e `pidgin-otr`.

## 20.2 Avviare Pidgin

Per aprire il software di messaggistica istantanea, apriamo la panoramica attività premendo il tasto ⊞ (⌘ su Mac), quindi digitando `pidgin` e infine facendo clic su "Pidgin Internet Messenger".

## 20.3 Configurare un account

Quando apriamo Pidgin, se non è già configurato alcun account, una finestra proporrà di aggiungerne uno nuovo.
Per configurare un nuovo account, facciamo clic sul pulsante "Aggiungi…".
Si aprirà una finestra "Aggiungi account". Se disponiamo già di un account di messaggistica istantanea, forniamo le informazioni necessarie di questo account, iniziando col selezionare il "Protocollo" che desideriamo utilizzare. Altrimenti, dovremo creare un account, come spiegheremo qui sotto.

## 20.4 Creare un account di messaggistica istantanea

Se non abbiamo un account di messaggistica istantanea, ora è il momento di crearne uno. Come per un account di posta elettronica, saranno richiesti un nome utente e una passphra-

4 Tomo I, cap. 15
5 Tomo I, cap. 16.3

se[6]. Per evitare di utilizzare sempre la stessa o rischiare di dimenticarla, è possibile usare un password manager[7].
Alcuni provider di indirizzi email, come il collettivo statunitense Riseup, offrono un account di messaggistica istantanea[8] a chiunque disponga di un indirizzo email, proprio come un account Facebook dà accesso alla messaggistica istantanea del sito Facebook Messenger.
Possiamo utilizzare i server di comunità in cui l'iscrizione è libera. Ad esempio, sul sito jabberfr.org[9] è disponibile un elenco di server XMPP[10] liberi. Una volta scelto un server e inserite le informazioni necessarie[11] nella finestra "Pidgin", selezioniamo la casella "Crea il nuovo account sul server".
È anche possibile connettersi ai server di protocollo IRC[12] senza avere un account[13].

## 20.5 Cifrare la connessione al server XMPP

Di default, Pidgin configura il nuovo account per cifrare la comunicazione con il server XMPP. Se il certificato è firmato da una Certification Authority [14], la connessione si svolgerà senza problemi e Pidgin salverà il certificato del server XMPP nella sua configurazione.
Se il certificato del server non è firmato, o se per qualche ragione Pidgin non può verificarne l'autenticità, sarà allora ne-

6 Tomo I, cap. 12
7 Cap. 21
8 https://help.riseup.net/it/chat/
9 Lista di server XMPP comunitari: modeci.vado.li
10 Wikipedia, *Extensible Messaging and Presence Protocol*.
11 Per maggiori dettagli, consultare il sito di Linuxpedia: cupubi.vado.li
12 Wikipedia, *Internet Relay Chat*.
13 #irchelp, *IRC Networks and Server Lists* [https://www.irchelp.org/networks/].
14 Cap. 6.4.2

cessario applicare le stesse tecniche di verifica per un certificato nel browser web[15], altrimenti un avversario potrebbe usurpare l'identità del server[16].
In questo caso, la prima volta che accediamo, Pidgin mostrerà una finestra che ci chiede se vogliamo "Accettare il certificato per esempio.org?". Spiegherà anche il motivo per cui non ha voluto accettare il certificato ("Il certificato è autofirmato. Non può essere verificato automaticamente", se ad esempio il certificato non è firmato da una Certification Authority. Cliccando su "Visualizza certificato...", Pidgin mostrerà il suo fingerprint[17], permettendoci di verificarlo[18].

## 20.6 Attivare il plugin Off the Record

Nel menu "Strumenti di Pidgin", facciamo clic su "Plugin". Troviamo la riga "Messaggi riservati 'Off-the-Record'" e selezioniamo la casella corrispondente per attivare il plugin. È possibile, cliccando su "Configura il plugin", scegliere alcune opzioni come "Non archiviare conversazioni OTR".

## 20.7 Impostare una conversazione privata

### 20.7.1 Aggiungere un contatto o unirsi a una stanza virtuale

A seconda della nostra situazione, dovremo aggiungere il contatto con cui vogliamo parlare in Pidgin, o dovremo unirci alla stanza in cui trovarlo.

---

15 Cap. 16
16 Cap. 6.4.1
17 Tomo I, cap. 5.2
18 Cap. 16

**Aggiungere un contatto**
Per aggiungere un contatto in Pidgin, facciamo clic su "Contatti" nella barra dei menu del software e andiamo su "Aggiungere un contatto...". Inseriamo quindi le informazioni corrispondenti del nostro contatto e clicchiamo su "Aggiungi" per terminare.
Ora dobbiamo solo aspettare che quella persona sia online.

**Entrare in una stanza**
Se invece vogliamo entrare nella stanza in cui probabilmente si troverà la persona con cui intendiamo conversare, clicchiamo su "Contatti" nella barra dei menu del software e andiamo su "Partecipa a una discussione...". Nella stessa maniera, inseriamo le informazioni necessarie e infine clicchiamo su "Chat".

### 20.7.2 Iniziare una conversazione privata

Per avviare una conversazione privata, facciamo doppio clic su un nome nella colonna di destra della finestra di una stanza in cui ci si trova oppure facciamo clic sul nome del nostro interlocutore nella finestra principale di Pidgin. Si aprirà una finestra di conversazione. Clicchiamo allora sul menu "OTR" → "Avvia una conversazione privata".
Se è la prima volta che si utilizza OTR con questo account, Pidgin genererà una chiave privata e mostrerà una finestra "Genera chiave privata". Questa chiave è univoca per un determinato account. Se disponiamo di più account di messaggistica istantanea, avremo quindi più chiavi. Quando saremo avvisati che la chiave è stata generata, si può chiudere questa finestra facendo clic su "Convalida".
Pidgin mostrerà allora che "Alice non è stata ancora autenticata. Dovreste autenticare questo contatto". Ciò significa che la nostra conversazione è cifrata, ma un avversario potrebbe

fingere di essere Alice[19]. Per essere sicuri di parlare con Alice, dobbiamo autenticarla.

### 20.7.3 Autenticare un corrispondente

Per autenticare un corrispondente, è necessario essersi preventivamente messi d'accordo su un segreto, o disporre di un mezzo di comunicazione diverso dalla messaggistica istantanea, considerato sicuro. Questo mezzo può essere una conversazione a viva voce, un'email cifrata, ecc.
OTR offre tre modi per autenticare un contatto:

- tramite domanda-risposta: definiamo una domanda e la sua risposta. La domanda verrà poi posta al nostro corrispondente;
- tramite segreto condiviso: viene domandato un segreto noto solo ai due interlocutori per verificare che vi sia un dialogo proprio con la persona attesa;
- grazie alla verifica manuale del fingerprint: verifichiamo che il fingerprint della chiave della persona con cui stiamo per avere una conversazione cifrata sia lo stesso che ci è stato fornito tramite un mezzo *autenticato*.

Una volta scambiati i segreti, le domande-risposte o i fingerprint, clicchiamo sul menu "OTR" → "Autentica contatto". Scegliamo il metodo di autenticazione in "Come desideri autenticare il tuo contatto?", quindi rispondiamo alle domande. Infine, facciamo clic su "Autentica".
Se l'autenticazione ha esito positivo, lo stato della conversazione cambierà in "Privato", il che significa che non è solo cifrato, ma anche autenticato.
Se si utilizza un sistema non-live o se abbiamo abilitato la per-

19 Cap. 6.4.1

sistenza[20] Pidgin in Tails, questo passaggio di autenticazione deve essere effettuato solo la prima volta per ogni contatto.

### 20.7.4 Terminare una conversazione

Una volta terminato il nostro dialogo, clicchiamo sul menu "OTR" → "Termina conversazione privata". Ciò cancella la chiave di cifratura temporanea generata per questa conversazione dalla RAM del computer. Anche se un avversario ottenesse le nostre chiavi private, non avrebbe accesso alla chiave che gli consentirebbe di decifrare la conversazione a posteriori.

20 Tomo I, cap. 14.5

# 21 | Gestire le password

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 15 a 30 minuti.

Quando ci creiamo un indirizzo di posta, un account su un sito web, ecc. questo account generalmente è protetto tramite una password. È importante non utilizzare la stessa password per accedere a servizi che hanno dei livelli di sicurezza differenti, per esempio una casella di posta e un account su un sito di scacchi online.
È anche importante non utilizzare la stessa password neanche per identità contestuali diverse[1], per evitare che la compromissione di una comprometta anche le altre.
Ci sono due buone scuole di pensiero riguardo alla gestione delle password:

- scegliere e ricordare una passphrase diversa per ogni uso;
- generare in modo casuale le varie password e salvarle in un password manager protetto da una passphrase robusta che ci dovremo ricordare.

## 21.1 Scegliere una buona password

La prima scuola ha il vantaggio di non aver bisogno di alcun supporto di archiviazione: le password sono sempre con

1 Cap. 5.1

noi. Se scegliamo questa via, consultiamo il capitolo Scegliere una buona password[2]. Lo svantaggio è che quando gli account si moltiplicano, di pari passo con le identità contestuali, può succedere che anche le password da ricordare diventino molte.

## 21.2 Utilizzare un password manager

La seconda scuola in questo caso può venirci in aiuto. In pratica avremo una passphrase da ricordare per ciascuna identità e il nostro password manager si farà carico di conservare tutte le varie password legate a quell'identità. Questo può avvenire sia su un sistema Debian cifrato[3] che su un sistema live amnesico[4] utilizzando la persistenza[5].

### 21.2.1 Installare il password manager

Utilizzeremo il password manager KeePassX. Se sul nostro sistema non è già presente, installiamo il pacchetto[6] KeePassX. Su Tails lo troveremo installato già di default.

### 21.2.2 Lanciare KeePassX

Premere il tasto (⌘su Mac) per accedere alla vista d'insieme, poi scrivere `keepassx` e cliccare sull'icona di KeePassX.

2 Tomo I, cap. 12
3 Tomo I, cap. 15
4 Tomo I, cap. 14
5 Tomo I, cap. 14.5
6 Tomo I, cap. 16.3

### 21.2.3 Creare e salvare un database delle password

Un database (db) delle password è un insieme di password che vengono salvate dentro uno stesso db di KeePassX cifrato con una passphrase associata.
Se scegliamo di usare KeePassX dentro Tails, dovremo prima attivare la persistenza[7] e scegliere l'opzione "Dati personali".
Innanzi tutto dobbiamo creare un nuovo db delle password e salvarlo per poterlo poi riutilizzare nelle future sessioni di lavoro. Apriamo il menu "Database", poi clicchiamo su "Nuovo database". Apparirà una finestra e ci chiederà di "Cambiare la chiave principale". Dal momento che stiamo creando un nuovo database in realtà si tratta di creare una nuova chiave, piuttosto che cambiarla. La passphrase che ci verrà chiesto di scegliere servirà a decifrare il database delle password. Scriviamo due volte la passphrase dentro le caselle corrispondenti, poi clicchiamo su "OK".
Per salvare il db delle password appena creato clicchiamo di nuovo sul menu "Database" e poi su "Salva database". Dentro la casella "Nome del file" scrivere `keepassx`. Se stiamo utilizzando Tails, selezioniamo Persistent nell'elenco delle cartelle a sinistra. Altrimenti va bene la scelta di default. Infine "Salva".
Visto che questo database conterrà le nostre password, è importante scegliere una passphrase[8] robusta e ricordarsi di fare regolarmente una copia di backup del database[9].

### 21.2.4 Generare e salvare una password casuale

KeePassX consente anche di generare delle password casuali più robuste di quelle che potrebbero venire in mente a noi.

7 Tomo I, cap. 14.5
8 Tomo I, cap. 12
9 Tomo I, cap. 19

All'interno di KeePassX, clicchiamo nel menu "Voci", poi su "Aggiungi nuova voce". Riempire le caselle che ci servono. Quando arriviamo al campo "Password", clicchiamo sul pulsante "Gen." che sta sulla stessa riga della casella "Ripeti".
Si aprirà una sezione che contiene diverse opzioni per generare una password.
Preferibilmente scegliamo lettere minuscole, maiuscole e cifre, aumentiamo il numero dei caratteri (minimo 32), perché tanto non dovremo ricordarceli. I caratteri speciali invece, sono a volte fonte di problemi su alcuni programmi o siti

.
Clicchiamo su "Accetta" e poi su "OK".
A questo punto clicchiamo nel menu "Database" e poi su "Salva database".

### 21.2.5 Aprire e sbloccare un database delle password

Se vogliamo utilizzare un db delle password che abbiamo salvato in precedenza, dobbiamo prima sbloccarlo. Per farlo lanciamo KeePassX. Se trova in automatico un database vi aprirà una finestra chiedendovi la chiave principale di sblocco del db. Altrimenti cercate il database in questione cliccando sul menu "Database" e poi su "Apri database". Scriviamo la passphrase associata al db che vogliamo sbloccare e clicchiamo su "OK".
Se abbiamo sbagliato password, ci apparirà un messaggio d'errore:

> Errore
> Impossibile aprire il database.
> Chiave errata o file del database danneggiato.
> Clicchiamo su OK e riproviamo.

### 21.2.6 Utilizzare una password salvata

Dopo aver aperto e sbloccato il database delle password, possiamo utilizzare le varie password che sono salvate al suo interno.
Per utilizzare un account tra quelli salvati selezioniamolo dall'elenco. Andiamo sulla finestra che ci serve e clicchiamo sulla casella utente. Torniamo poi su KeePassX, clicchiamo su "Voci", poi scegliamo "Esegui Auto-type". A questo punto KeePassX si minimizzerà automaticamente nella barra delle applicazioni.

⚠ *Attenzione*: l'auto-type rischia di farci fare anche dei grandi pasticci, per esempio incollare la nostra password dentro una chat... Dobbiamo fare molta attenzione a dove abbiamo cliccato e posizionato il cursore prima di lanciare l'auto-type. È possibile che questo metodo di riempimento non funzioni in automatico su tutti i tipi di interfaccia. In questo caso possiamo cliccare con il destro sull'account selezionato in precedenza, scegliere "Copia nome utente", poi cliccare con il destro dove dobbiamo incollarlo e infine scegliere "Incolla". Stessa cosa per la password.

# 22 | Usare OnionShare

I software evolvono, per questo è vivamente consigliato utilizzare la versione più aggiornata di questa ricetta, che troverete in francese e in italiano sui siti della Guida https://guide.boum.org/ e https://numerique.noblogs.org/

Durata: da 5 a 10 minuti.

Per mettere a disposizione di altre persone uno o più file, è possibile farli ospitare su di un web server[1].
Tuttavia non c'è nessuna ragione per fidarsi a priori delle persone che si occupano di quel server. Se preferiamo evitare di doverci affidare a terzi, possiamo ospitarci da soli i file attraverso un Onion Service di Tor[2]. Questa scelta ha come altro vantaggio quello di proteggere fortemente la localizzazione del server che ospita i file, server che in questo caso è il nostro stesso computer. Non bisogna però dimenticare che questo sistema di anonimizzazione non è infallibile[3].
Per mettere in atto questo metodo utilizzeremo il software OnionShare, che permette con pochi clic di creare un Onion Service e di ospitarci sopra i file che vogliamo.

## 12.1 Utilizzare OnionShare dentro Tails

Al momento in cui scriviamo, non è semplice utilizzare OnionShare su Debian, per questo motivo spiegheremo unicamente il suo utilizzo con Tails.

1 Cap. 15
2 Cap. 7.1.3
3 Cap. 7.3

OnionShare è installato di default su Tails. Possiamo quindi seguire la documentazione ufficiale di Tails, che è disponibile su qualunque DVD o penna USB di Tails, senza neanche doverci connettere a internet.
Cominciamo avviando Tails[4]. Sul Desktop clicchiamo sull'icona della documentazione di Tails. Nel menu a destra clicchiamo su "Documentazione". Si aprirà un indice nel quale dobbiamo cercare la sezione "Connettersi a internet in modo anonimo" per poi cliccare su "Condividere file con OnionShare": ecco le istruzioni da seguire.

4 Tomo I, cap. 14.4

Per il grande aiuto e sostegno nella realizzazione dei due volumi dell'edizione italiana della *Guida all'Autodifesa Digitale* ci teniamo a ringraziare: Pinke, LaSoviet, boyska tutto minuscolo, Marcav, l'hacklab fiorentino If_Do e gli hacklab di tutta Italia, il nEXt Emerson, la stupenda comunità di Hackmeeting, Radio Wombat, la Ciurma Pirata e gli smanettoni di tutto il mondo uniti.

# INDICE